The Computer & Internet Lawyer

Volume 37 ▲ Number 4 ▲ APRIL 2020

Ronald L. Johnston, Arnold & Porter, LLP, Editor-in-Chief

Features

Current Developments

By Steven A. Meyerowitz

. . . and more!

Wolters Kluwer

Board of Editors

Editorial Office

26910 Grand Central Pkwy. #18R
Floral Park, NY 11005
smeyerowitz@meyerowitzcommunications.com

Business Office

28 Liberty Street
New York, NY 10005
(212) 771-0600

The COMPUTER & INTERNET *Lawyer*

Cite as The Computer & Internet Lawyer, Vol. 37, No. 4. [page].

The Computer & Internet Lawyer (USP 729-750) (ISSN 0742-1192) is published monthly and bimonthly for July/August and November/December issues for $1,215 for one year by Wolters Kluwer at 28 Liberty Street, New York, NY 10005. Postmaster: Send address changes to *The Computer & Internet Lawyer*, 7201 McKinney Circle, Frederick, MD 21704. Send editorial correspondence and submissions by email to smeyerowitz@meyerowitzcommunications.com. To subscribe, call 1-800-638-8437 or order online at *www.WoltersKluwerLR.com*. For customer service, call 1-800-234-1660.

Permission requests: For information on how to obtain permission to reproduce content, please go to *www.WoltersKluwerLR.com/policies/permissions-reprints-and-licensing.* **Purchasing reprints:** For customized article reprints, please contact *Wright's Media* at 1-877-652-5295 or go to the *Wright's Media* Web site at *www.wrightsmedia.com.*

The Battle Over Encryption

By Brandon H. Graves

Since encryption was developed, governments have sought to break it. Initially, these efforts were focused on breaking encryption used by other governments, as sophisticated encryption was beyond the capability of most private citizens.

Today, however, practically unbreakable encryption is available to almost everyone, in devices we carry around in our pockets. Wide availability of strong encryption has been a boon to consumers, whose digital data enjoys greater protection today as a result.

It creates problems for law enforcement, however, which may be unable to access information on phones or computers that contain evidence essential to their investigation of criminal behavior. Governments, on behalf of both law enforcement and national security entities, have asked companies to create "backdoors" in encryption algorithms to enable government access to protected information in time of need.

Tech companies, however, have uniformly resisted these requests, arguing that backdoors could undermine the very protection that consumers have come to expect. For this reason, the companies and privacy advocates have long resisted efforts by government to mandate backdoors.

Government calls for encryption backdoors have recently resumed, due in part to the extension of end-to-end encryption to more products and the U.S.-U.K. Bilateral Data Access Agreement, the first Executive Agreement under the CLOUD Act.

Why End-to-End Encryption?

Companies can use two methods to encrypt consumers' messages:

- The first, more traditional method is to encrypt the message from the sender to the company, decrypt the message for processing, and re-encrypt for transmission to the recipient. This, of course, permits the company to see the message, and even store it on central servers for later retrieval.
- The second method, end-to-end encryption, encrypts the message on the sender's device, and only decrypts it at its destination, on the receiver's device. If the message is stored at the company at all, it is stored in an encrypted format that the company cannot decrypt.

End-to-end encryption offers a number of benefits to consumers, and companies have started highlighting end-to-end encryption as a selling point in their offerings. Properly implemented, end-to-end encryption prevents companies from viewing customer data. This means that the companies can't use the customers' messages to build profiles, target advertising, or re-identify de-identified information.

Indeed, end-to-end encryption has potential to mitigate or eliminate many end-user privacy concerns.

End-to-end encryption also helps consumers prevent third parties, including governments, from accessing private conversations. This has been touted as critical for activists under repressive regimes who are seeking freedoms that many take for granted. But it can also assist criminals in avoiding law enforcement.

Why Can't Companies Give Law Enforcement the Keys?

Many people have asked why companies cannot develop backdoors to their encryption solutions and provide access exclusively to law enforcement, thereby providing the privacy benefits while eliminating the costs to law enforcement. For many reasons, this is not likely to work.

- First, no encryption scheme is perfect. In theory, we have developed encryption that is so strong that it cannot be broken until the heat death of the universe (or the advent of quantum computing). Unfortunately, in practice we often find out that the implementation of the encryption is flawed.[1]

  Encryption algorithms are difficult to implement.

  To implement an algorithm that permits a reliable, secure backdoor is infinitely harder. So it is likely that the encryption itself will have exploitable flaws.

Brandon H. Graves is counsel in the Washington, D.C., office of Davis Wright Tremaine LLP. He may be contacted at *brandongraves@dwt.com*.

- Second, in practice the process of implementing the backdoor will itself be likely flawed. Threat actors often find a way to exploit any backdoor reliable enough for law enforcement use. These backdoors will be high-value targets for criminals, who could either exploit the backdoors or sell them to other criminals.For example, some years ago, the cell phones of many Greek government officials were tapped by means of unauthorized use of the wiretapping capabilities that, by law, are built into traditional communications networks.

- Third, it will be difficult for companies to resist demands for the keys from authoritarian regimes once the backdoors are built. Because these regimes exercise governmental authority in their respective countries, they have the legal power to demand that companies wishing to do business in their country turn over the keys to any backdoor that has been developed.And, of course, the broader the distribution of these keys, the more likely they are to fall into the wrong hands, subjecting communications to unauthorized decryption.

- Finally, some privacy advocates are concerned that U.S. law enforcement will use data sharing agreements to get around the Fourth Amendment. Backdoors into consumer encryption will only facilitate such access.

What Should We Do?

Those who call for backdoors, both for communications and the devices used to communicate, often claim dire consequences will ensue without them, but provide little factual support for their claims. Although it is possible for criminals to use encrypted communications to elude law enforcement, it is far from clear how often encryption actually prevents law enforcement from solving cases.

At least one law enforcement official has claimed to have a number of encrypted devices sitting useless in evidence, but fails to state how many prosecutions were thwarted because of encryption.The most famous example of an encrypted device that posed problems for law enforcement was resolved without the company at issue having to implement a backdoor (the FBI paid a "mysterious third party" who unlocked the device). And the FBI never disclosed what benefit it got from accessing the device after it bypassed the encryption.

Law enforcement access to encrypted information is not a simple problem to solve. Encryption backdoors could potentially have an adverse impact on consumers' data security. Therefore, all potentially affected parties should weigh in on whether the potential cost is worth the purported benefits.

Note

1. Mark M. Christiansen, Ken R. Duffy, Flavio du Pin Calmon, and Muriel Medard, "Brute force searching, the typical set and Guesswork," *available at https://arxiv.org/pdf/1301.6356.pdf.*

Ninth Circuit Rejects LinkedIn's Efforts to Block Web-Scraping of Member Public Profiles

By Lee Johnston

Social media companies (SMCs) are constantly working to leverage data they gather from customers to develop new, innovative products and effective advertising strategies to market those products. At the same time, SMCs face threats from competitors seeking to harvest and exploit the publicly-available customer data hosted on SMC servers.

On the technology side, SMCs employ increasingly sophisticated artificial intelligence (AI)-based software to prevent automated bots and web crawlers from accessing and scraping customer data from SMC websites. And, under the auspices of enforcing their own proprietary rights and their customers' privacy rights, SMCs have asserted a variety of legal claims – ranging from common law trespass and breach of contract theories to federal copyright and Computer Fraud and Abuse Action (CFAA) claims – in an effort to shut down, or at least deter, their competitors' efforts to access and "scrape" SMC customer data.

As judges have gained a better understanding of the technology and legal issues in these cases, the viability of some of these claims has been circumscribed.[1]

Nevertheless, SMCs have largely been on the offensive in this battle, primarily due to their ability to outspend their competitors, which are often start-ups lacking the resources for extended legal battles. The recent decision by the U.S. Court of Appeals for the Ninth Circuit in *hiQ Labs, Inc. v. LinkedIn Corp.*,[2] however, suggests a more favorable future for web scraping in general, and specifically highlights the effectiveness of smaller competitors' strategy of "taking the battle" to larger SMCs rather than waiting to be sued.

hiQ Labs v. Linkedin Corp.

In *hiQ Labs*, the Ninth Circuit affirmed the trial court's preliminary injunction barring LinkedIn from blocking or otherwise hindering hiQ's ability to "scrape" LinkedIn users' public profiles. The underlying dispute in *hiQ Labs* centered on hiQ's data analytics business model, which depends exclusively on its ability to scrape LinkedIn's users' public profile information. Using automated bots to harvest LinkedIn users' name, job title, work history and skills, hiQ applies a proprietary algorithm to this data to yield "people analytics," which it then sells to business clients to allow them to identify employees at the greatest risk of being recruited away, as well as to identify skill gaps in an employer's workforce.

LinkedIn took issue with hiQ's activities, especially because LinkedIn itself sought to develop and market its own skill-based predictive analytics product (Talent Insights) based on users' profiles. In May 2017, LinkedIn sent hiQ a cease-and-desist letter, asserting that hiQ had violated LinkedIn's terms of use agreement, and that any future access of LinkedIn data would subject hiQ to liability under the CFAA, the Digital Millennium Copyright Act (DMCA), California Penal Code Section 502(c), and the California common law of trespass.

Rather than taking a defensive posture, hiQ went on the offensive and filed a pre-emptive lawsuit seeking a declaration that it was legally entitled to scrape LinkedIn user profiles and that LinkedIn could not lawfully invoke the federal and state laws identified in its cease-and-desist letter. hiQ also went a step further, and sought an injunction prohibiting LinkedIn from erecting technological barriers to hiQ's automated bots. By doing so, hiQ effectively pivoted the Court's analysis, and instead of being seen as an Internet parasite, hiQ was able to successfully argue that it was the victim of LinkedIn's heavy-handed, anti-competitive tactics.[3] And, by posturing the case as one requiring immediate injunctive relief, hiQ highlighted its strongest argument – that LinkedIn's actions would destroy hiQ's business – and reduced its burden of proof on establishing the likelihood of success on the merits of its legal claims.[4]

hiQ's high-risk/high return legal strategy paid off, primarily due to (1) LinkedIn's inability to argue plausibly that its users' privacy interests were harmed by hiQ's conduct, and (2) the court's concern that a finding of liability under the CFAA would expand the statute's reach beyond what Congress intended.

Lee Johnston, a partner in the Denver office of Haynes and Boone, LLP, has a national trial practice that includes patent, copyright, trademark, and trade secret litigation. Mr. Johnston may be reached at *lee.johnston@haynesboone.com*.

First, as to privacy concerns, both the trial court and Ninth Circuit found it significant that LinkedIn had no proprietary interest in the factual information contained in its users' online profiles. LinkedIn users, not LinkedIn, "owned" this factual data, and voluntarily chose to make their profiles available to the public. Indeed, LinkedIn's own privacy policy stated that "any information you put on your profile and any content you post on LinkedIn may be seen by others," and warned users not to "post or add personal data to your profile that you would not want to be public."[5] Moreover, LinkedIn's professed privacy concerns were undermined by the fact that LinkedIn allowed other third-parties to access user data without its members' knowledge or consent.

The trial court and the Ninth Circuit also expressed serious concerns about LinkedIn's CFAA argument that hiQ's violation of the LinkedIn website terms of use provisions and disregard of LinkedIn's subsequent cease-and-desist letter constituted violations of the CFAA's prohibition against computer access "without authorization." As the trial court noted, LinkedIn's interpretation of the CFAA would permit a website owner to revoke the "authorization" of any person at any time, for any reason, and then pursue civil and criminal penalties against that person for merely *viewing* the website – an outcome which the trial court characterized as "effectuating the digital equivalence of Medusa."[6] According to the trial court, allowing a private entity to effectively criminalize access to publicly viewable information, without any consideration of the website owner's reasons for denying access or an individual's possible justification for ignoring the website owner's denial of access, would be "particularly pernicious" to healthy competition and the public's right to information.[7]

The Ninth Circuit agreed, holding that the CFAA's prohibition against accessing a protected "without authorization" must be viewed in the context of the three types of information which exist on computers:

- Information for which access is open to the general public and permission is not required;
- Information for which authorization is required and has been given; *i.e.*, username and password authentication; and
- Information for which authorization is required but has not been given (or, in the case of the prohibition on exceeding authorized access, has not been given for the part of the system accessed.)

According to the Ninth Circuit, the information which hiQ accessed and "scraped" fell into the first category of "computer information" for which no permission was required. As such, the court found that liability under the CFAA could not be based on LinkedIn's digital user agreement or the express revocation of hiQ's access rights contained in LinkedIn's cease-and-desist letter.[8]

The Renewed Importance of Requiring Password Authentication of Customer/User Data for CFAA Liability

The Ninth Circuit's decision underscores the importance of user authentication systems in determining whether liability under the CFAA will be triggered. In *U.S. v. Nosal* ("*Nosal II*"),[9] the Ninth Circuit held that a former employee whose computer access rights had been terminated when he left his employer, but who had then used current employees' login credentials to access company computers and collect confidential information, had acted "without authorization" in violation of the CFAA.[10] Similarly, in *Facebook v. Power Ventures, Inc.*,[11] the Ninth Circuit held that Power Ventures, Inc., a social networking website that aggregated social networking information from multiple platforms, had violated the CFAA by accessing Facebook users' password-protected data (e-mail/contact information) and then using that data to send mass e-mail messages as part of a promotional campaign.[12]

Using its newly-articulated analytical framework, the Ninth Circuit in *hiQ Labs* observed that, unlike LinkedIn users' public profiles, the computer information being accessed in *Nosal II* and *Power Ventures* was "plainly" the type where authorization was generally required; that is, requiring password authentication, and that authorization had either never been given or had been revoked:

> It is likely that when a computer network generally permits public access to its data, a user's accessing that publicly available data will not constitute access without authorization under the CFAA. The data hiQ seeks to access is not owned by LinkedIn and has not been demarcated by LinkedIn as private using . . . an [username/password] authorization system.[13]

LinkedIn's Anticipated Trip to the U.S. Supreme Court

Following its unsuccessful attempt to have the Ninth Circuit revisit its decision [14] LinkedIn has indicated that it will seek the U.S. Supreme Court's review and reversal

of the Ninth Circuit's *hiQ Labs* decision. In papers filed with the Court on January 22, 2020, LinkedIn framed its anticipated appeal as one:

> present[ing] a recurring and important question on which the courts of appeals are divided: whether an entity that deploys anonymous computer "bots" that circumvent technical barriers and mass-harvests individuals' personal data from computer servers – even after the entity's permission to access those servers has been expressly denied by the website owner – "intentionally accesses a computer without authorization" under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030(a)(2).[15]

LinkedIn's Petition for Writ of Certiorari is due for filing at the U.S. Supreme Court on March 6, 2020, and it remains to be seen whether the Court will even elect to hear the case.[16]

While the outcome on LinkedIn's anticipated appeal is uncertain, one thing remains clear: the battle between SMCs and "scrapers" is far from over. Even if the U.S. Supreme Court leaves intact the Ninth Circuit's restrictions on the use of the CFAA in these types of cases, the hiQ decision makes it clear that SMCs and other online entities which view themselves as victims of data scraping are not without other legal recourse. As the Ninth Circuit itself pointed out, common law claims (for example, trespass to chattels, unjust enrichment, conversion, breach of contract and breach of privacy) and statutory claims (for example, copyright infringement and misappropriation of trade secrets) may still be available to website owners like LinkedIn to prevent, or at least slow down, unwanted data scraping activities.[17]

Notes

1. *See, e.g., TicketMaster.com v. Tickets.com*, 2003 WL 21406289 (C.D. Cal. March 7, 2003) (dismissing copyright and trespass to chattels claims where only factual, publicly-available data was "scraped" from TicketMaster's website and re-published by Tickets.com in a different format, and Tickets.com's use of web crawler did not impact or interfere with the functionality of Ticketmaster.com's server); *Sandvig v. Sessions*, 315 F.Supp.3d 1 (D.D.C. 2018) (First Amendment interests were implicated and thus called into question the criminal prosecution of journalists under the Computer Fraud and Abuse Act for their use of automated bots to scrape data in breach of a website's terms of use agreement).
2. 938 F.3d 985 (9th Cir. 2019).
3. *Id*. at 998 (observing that LinkedIn's conduct "may well not be 'within the realm of fair competition.'") (citations omitted).
4. *See Alliance for the Wild Rockies v. Cottrell*, 632 F.3d 1127, 1131 (9th Cir. 2011) (adopting a sliding scale approach and holding that where the party seeking an injunction establishes irreparable harm is virtually certain, it need only demonstrate that there are "serious questions going to the merits" of its legal claims).
5. *hiQ Labs*, 938 F.3d at 994.
6. *hiQ Labs v. LinkedIn Corp.*, 273 F.Supp.3d1099, 1110 (N.D. Cal. 2017).
7. *Id*. at 1112.
8. *hiQ Labs,* 938 F.3d at 1002.
9. *U.S. v. Nosal*, 844 F.3d 1024 (9th Cir. 2016) ("NOSAL II").
10. *Nosal II*, 844 F.3d at 1038.
11. *Facebook v. Power Ventures, Inc*, 844 F.3d 1058 (9th Cir. 2016).
12. *Id*. at 1062-63.
13. *hiQ Labs,* 938 *F.3d* at 1003–04.
14. *See hiQ Labs, Inc. v. LinkedIn Corp.,* Case No. 17-16783 (9th Cir.), Dkt No. 89 (Order denying LinkedIn's Petition for Rehearing and Petition for Rehearing En Banc).
15. *See LinkedIn Corp. v. hiQ Labs, Inc.,* No. 19A819 (U.S. Supreme Court) (LinkedIn's Application for Extension of Time within which to File a Petition for a Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit).
16. From 2014 to 2017, the percentage of writs of certiorari in civil cases granted by the U.S. Supreme Court has ranged from 2.0 percent to 3.4 percent. *See* "Success Rate for a Writ of Certiorari to the Supreme Court," Supreme Court Press (https://supremecourtpress.com/chance_of_success.html).
17. *hiQ Labs,* 938 F.3d at 1004.

A Brief History of Memory Forensics, How Volatile Computer Memory Works, and Malware and Volatile Memory

By Michael J. Hannon

Digital evidence created and stored on computers, smartphones, and other digital devices has become increasingly important in criminal investigations and trials.[1] Even relatively routine events can generate digital evidence.[2] For decades, digital evidence created by computer activity and stored on hard drives was the focus of criminal investigations and civil litigation. Computer forensic experts developed tools, procedures, techniques, and practices to capture and preserve digital evidence on hard drives for later analysis. These tools and methods are employed to preserve potential digital evidence in as pristine condition as possible.[3] Preventing any alteration to digital evidence is seen as a fundamental goal so the evidence can ultimately be used in legal proceedings.[4]

The March 2020 issue of *The Computer & Internet Lawyer* contained the first in a series of articles by this author addressing issues relating to volatile computer memory evidence, entitled "Volatile Computer Memory Evidence: Forensics Issues." This article continues the discussion, with a brief history of memory forensics, some basic technical details about volatile computer memory, and initial thoughts on malware and volatile memory.

Brief History of Memory Forensics

The focus on preserving potential evidence on computer hard drives at the expense of potential evidence in volatile memory is primarily the result of several factors. A major factor that drove traditional digital forensics to focus on preserving and analyzing potential evidence on computer hard drives was the lack of tools, techniques, and knowledge needed to capture volatile memory. As a result, protocols and techniques that focused on preserving and analyzing evidence on computer hard drives became established doctrine.

Michael J. Hannon, the associate director for access services and digital initiatives at the University of Minnesota Law Library, may be contacted at *mhannon@umn.edu*.

An important milestone in the development of volatile memory forensics came from the 2005 Digital Forensic Research Workshop (DFRWS).[5] That year, the DFRWS annual challenge tasked forensic practitioners to perform a:

> thorough analysis of a Windows memory sample. This led to the creation of several memory analysis tools, including KntTools (Garner, 2005), MoonSols (Suiche, 2007), the FATKit (Petroni et al., 2006), VolaTools (Walters and Petroni, 2007), and Volatility (The volatility framework, 2016). In the years since, several powerful open source frameworks as well as commercial analysis tools have been developed.[6]

Since those early days of memory forensics, sophisticated tools and techniques have been developed and a commensurate body of knowledge has been created.[7] This has led to memory forensics becoming an accepted and important branch of digital forensics.[8]

However, even after volatile memory acquisition tools were developed, traditional computer forensic practice has prevailed to a significant extent for several reasons. Acquiring and analyzing volatile memory is more complex than traditional hard drive evidence.[9] It is a more specialized practice. In addition, because acquiring volatile memory requires that the target computer be running, volatile memory is constantly changing during the acquisition process. Moreover, some types of memory acquisition tool may need to run in volatile memory in order to capture it. This alters the volatile memory to a certain extent. And any change to the evidence violates a cardinal rule of digital forensics. Any alteration to digital evidence raises concerns about how judges and juries will perceive digital evidence in criminal prosecutions.

The development of tools, knowledge, and techniques to capture and analyze volatile memory has led to changes in some investigations when a running computer is encountered. It is increasingly likely that in some situations, some investigators will try to capture volatile memory before pulling the plug on a running

computer.[10] However, while there has been tremendous improvements in memory forensic tools, techniques, and knowledge over the past decade, it is still more difficult to acquire and analyze volatile memory than to create a mirror image of a computer hard drive. Although some sources state that RAM acquisition tools and techniques are simple enough for first responders to utilize when they encounter a running computer.[11] However, even if in some situations capturing volatile computer memory may be accomplished by first responders, analyzing volatile memory is still a specialized field requiring significant skill and knowledge.

Some Basic Technical Details About Volatile Computer Memory

Modern computers are incredibly complex. Volatile memory on a computer is as technically complex as anything on a computer. Acquiring and analyzing volatile memory can be very challenging. This section will provide a very basic overview of volatile memory.

When computer users are working at their computer, everything displayed on the screen, the software programs they are using (web browsers, word processors, videos, spreadsheets, games, etc.), and many other programs, program processes, and other technologies that the user might not be aware of are running in the memory of the computer. This type of memory is called Random Access Memory and is more often referred to as RAM.[12] Computer RAM is potentially very fragile because it requires constant electrical power to be maintained. For this reason, RAM is often referred to as volatile memory because everything running in RAM basically disappears when it loses electricity.[13] This type of temporary memory is also referred to as "dynamic" because it needs a constant supply of electricity to maintain data.[14] The most obvious way computer RAM loses electricity and RAM content disappears is for someone to pull the plug or shut the computer down.[15] The loss of potential evidence in RAM when a computer is shutdown is a permanent cost because "volatile data will be lost forever if not collected while the computer is running."[16] Significantly, potential evidence can persist in volatile memory for long periods of time on a running computer.[17]

Physical Memory

Digital forensic practitioners often refer to volatile computer memory (RAM) as "physical memory."[18] This is to contrast it with virtual memory (page or swap file discussed below) where a computer stores software programs that are open but not currently being used on a computer hard drive.[19] Volatile RAM enables a computer operating system to perform actions very rapidly which is important for computer performance. Accessing programs in RAM is many times faster than accessing programs from a hard drive.[20] In contrast to volatile memory which is constantly changing, everything else stored on a computer hard drive is static – closed software programs, files, browser histories. When a user clicks on or opens a software program or file (or the operating system opens a program or file) that is stored on the hard drive, it is opened up into volatile memory. Computer users interact with programs and files in volatile memory.

Although volatile memory dissipates very rapidly if not constantly supplied with electricity, researchers in 2008 revealed that data stored in volatile memory may not be lost immediately after a computer is shutdown.[21] This research has led to the development of several techniques that are generally referred to under the umbrella term "cold boot attack" which might enable an investigator to preserve volatile memory evidence if utilized very quickly after a computer is powered down.[22] The term "cold boot" comes from research that shows that if physical RAM chips are removed from a computer (and thus no longer have electricity to maintain data) but are immediately chilled to –50° C or colder, the RAM chips continue to hold data for much longer than they would at a normal temperature.[23] This can be done by spraying the RAM chips with aerosol propellant from cans used for cleaning electrical equipment.[24] Details about cold boot techniques are beyond the scope of this article due to the specialized nature, tools, and techniques needed to successfully perform a cold boot preservation of volatile memory.

Potential Evidence in Volatile Memory

Volatile memory is potentially a very important source of evidence because all activity on a running computer (human user activities or automatic computer operations) is conducted in volatile memory. Basically, every activity on a computer is running or was running at some point in the volatile RAM.[25] This includes any type of interaction between computers on the internet and also cyber-intrusions such as malware, hacking, and unauthorized access. This section will cover some basics of volatile memory on Windows computers but many of these same concepts apply to Apple computers. Some of the important evidence of activities in volatile memory on a running computer include:

- Processes and threads;
- Malware (including rootkit technologies);

- Network sockets, URLs, IP addresses;
- Open files;
- User generated content such as passwords, caches, and clipboards;
- Encryption keys;
- Hardware and software configuration; and
- Windows registry keys and event logs.[26]

Some of these activities such as open files, user generated content, and passwords are self-explanatory. A number of these other important activities are briefly explained below.

Processes

Software programs running on a computer are "executed" in RAM and "a process is a container for a set of resources used to execute a program."[27] A software program running on a computer has a presence in volatile memory, specifically in processes:

> A process is an instance of a program that has been executed in the system. Each process in memory has a private isolated memory space. A process contains the execution code and the data that is required to complete the execution of the code, such as files, DLLs, and user input. All this data and code are located in a memory space allocated for this process.[28]

Processes in volatile memory are proof of software programs running on a Windows computer, including malware, so processes are a major focus of memory forensics.[29] Evidence of currently running processes and evidence that closed processes were previously running can be obtained from volatile memory. On Windows computers, each process "is represented as an executive process, or EProcess, block. This EProcess block is a data structure in which various attributes of the process, as well as pointers to a number of other attributes and data structures (threads, the process environment block) relating to the process, are maintained."[30]

Threads

Threads are related to processes in that each process has one or more threads.[31] A thread is "the basic unit of CPU utilization and execution. . . . In memory forensics, thread data structures are useful because they often contain timestamps and starting addresses. This information can help you determine what code in a process has executed and when it began."[32] Analysis of processes and threads in volatile memory on a Windows computer can reveal important sources of evidence about computer activities if the RAM is analyzed or captured before the computer is shutdown:

> The Windows family of operating system records all of the metadata necessary to manage the processes currently being executed in physical memory. Even if a process exits its metadata may be retained in memory for weeks. The information stored in the metadata provides a snapshot of the processes and threads that are either currently or have recently executed on a system. As such an understanding [of] the common data structures utilised by Windows operating systems to manage the execution of processes is an important part of memory analysis.[33]

On a Windows computer, the user can see active processes that are currently running in memory by selecting the following keys on the computer keyboard at the same time: Control, Alt, Delete. This will bring up the Task Manager which will have a tab that displays active processes. If there are any programs loaded in memory such as browsers (Chrome, Firefox, etc.), Microsoft Office, video players, etc., there will be a process listed for each instance of that program.[34]

Malware And Volatile Memory

Malware is a catch-all term for any type of malicious program that infects a computer "'malware' generally describes computer programs written with the intent of being disruptive or damaging to a computer or computer user, and encompasses computer viruses, worms, and spyware."[35] There is an ever growing number of various types of malware that threaten the cybersecurity of individuals, businesses, and organizations. In 2019, AV-TEST GmbH, an independent IT security research institute in Germany, registered over 350,000 new malware and potentially unwanted applications every day.[36]

Traditional cybersecurity relies to a significant extent on signature-based detection which enables security tools such as anti-virus systems, firewalls, and forensics to detect and identify *known* malware by its signature. However, malware authors are aware of these security techniques so they are constantly devising new methods to evade signature-based malware security systems.[37] Sophisticated malware is constantly changing so security systems created to detect and protect against known threats are increasingly inadequate:

> [N]ew generation malware executables can modify their signatures or structures by applying obfuscation techniques like polymorphism, oligomorphism, metamorphism and encryption to bypass static analysis. For instance, metamorphic malware executables have ability to change their content, size, and signature by using disassembler, code analyzer, code transformer and assembler in order to create their mutants. Therefore, static methods can be ineffective to detect these new generation executables.[38]

Malware developers are creating and deploying increasingly sophisticated and destructive programs. For example, a technically advanced form of malware is "code injection" which "perform actions from within the context of another process. By doing so, the malware can force a legitimate process to perform actions on its behalf, such as downloading additional trojans or stealing information from the system."[39]

One of the most insidious and potentially destructive types of malware are rootkits, software exploits that take elaborate steps to remain hidden on a computer.[40] However, a rootkit must have some presence in volatile memory in order to run and exploit the victim computer. In 2006 a noted forensic expert termed this the "The Rootkit Paradox":

> All rootkits obey two basic principles: 1. They want to remain hidden. 2. They need to run. Taken together, these rules create a paradox. In order to remain hidden, the rootkit needs to minimize its footprint on the system. However, in order to run, the operating system, a deterministic process, has to be able to find and execute the rootkit. If a deterministic process like the operating system can find the rootkit, then an examiner can find it as well.[41]

Advanced types of malware have been created and deployed specifically to steal valuable data residing temporarily in computer memory. Some types of sophisticated malware are able to steal credit card information by "scrapping" it from the computer memory of computers used by merchants:

> Memory scrapers are a category of malware frequently used by attackers to obtain card numbers from the random access memory (RAM) of the Point-of-Sale (PoS) systems. Plentiful reports mention sophisticated malware employed in the perpetration of credit card frauds, ... The epitome of advanced PoS malware can be considered ChewBacca, . . . which dumps a copy of the running memory process, searches for credit card numbers and inputs the numbers found into a file. The communications between the infected devices and the perpetrators' server are accomplished through a network of encrypted relay systems. . . .[42]

In 2008 and 2009 hackers penetrated Wyndham Worldwide Corporation's computer systems three different times to steal confidential data including "payment card information from over 619,000 consumers, which . . . resulted in at least $10.6 million in fraud loss."[43] This significant security breach involved memory scraping programs:

> The FTC claims that Wyndham was unaware of the attack for two months until consumers filed complaints about fraudulent charges. Wyndham then discovered "memory-scraping malware" used in the previous attack on more than thirty hotels' computer systems. The FTC asserts that, due to Wyndham's "failure to monitor [the network] for the malware used in the previous attack, hackers had unauthorized access to [its] network for approximately two months." In this second attack, the hackers obtained unencrypted payment card information for approximately 50,000 consumers from the property management systems of 39 hotels.[44]

Numerous companies have been attacked by POS malware.[45] Sophisticated malware may have the ability to communicate with a Command and Control server to receive instructions or send stolen information.[46] In 2017 an advanced point-of-sale malware was discovered called LockPoS, which "at its core, functions as a memory scanner that scrapes the memory of currently running processes on the system, searching for credit card patterns and then sending them to a Command and Control server."[47]

One of the most dangerous types of malware or hacking exploit is ransomware. A successful ransomware attack obtains access to important computer files on a victim's system, encrypts the files to prevent access, and demands the victim pay a ransom to regain access. One of the most problematic ransomware attacks in the past few years is WannaCry.[48] WannaCry employs very strong encryption and communicates with a command and control server.[49] Volatile memory evidence may be an important part of analyzing ransomware and other malware attacks.[50]

As of 2018, one of the most insidious types of malware is Emotet, a sophisticated banking Trojan.[51]

According to the Cybersecurity and Infrastructure Security Agency (CISA) "Emotet continues to be among the most costly and destructive malware affecting state, local, tribal, and territorial ("SLTT") governments, and the private and public sectors."[52] In addition, it has evolved over time:

> Emotet uses a number of tricks to try and prevent detection and analysis. Emotet is polymorphic, which means it can change itself every time it is downloaded to evade signature-based detection. Moreover, Emotet knows if it's running inside a virtual machine (VM) and will lay dormant if it detects a sandbox environment.[53]

Fileless Malware

Some activities in volatile computer memory are never written to or stored on the hard drive. This includes some technically advanced forms of cybersecurity threats. Sophisticated malware is increasingly designed to hide evidence of the compromise on victim computers. Hackers and malware authors strive to minimize the malware's footprint on the computers they infiltrate to make it exceedingly difficult to discover and trace the intrusion. Malware that is able to operate without writing anything on the hard drive of the system that was compromised may only be vulnerable to memory forensics.[54] Sometimes these attacks are referred to as "memory resident" as evidence of their presence can only be found in the memory of the affected computer.[55] These sophisticated attacks do not store or leave any evidence on the hard drive.[56] Because of this, these advanced types of malware are often identified as "fileless malware."[57]

Cybersecurity experts sometimes describe these attacks as *non-malware* because the method of compromise does not install or use executable files. Instead, these attacks exploit and leverage existing parts of the operating system on the targeted computer. This is called "living on the land" because the attack does not bring and install its own executable files (that can be detected by cybersecurity software such as anti-virus programs) but infiltrates and exploits existing programs on the compromised computer.[58] Even if sophisticated malware leaves some traces on a computer hard drive, the traces may differ significantly from how the malware actually looks when it is active in memory on a running computer.[59]

Malware creators frequently target Microsoft Window systems by taking advantage of Powershell, a "command-line shell designed especially for system administrators."[60] Powershell is an important system administrator tool used for a variety of tasks.[61] The ability to exploit Powershell, a legitimate and powerful administrator tool, makes this a very dangerous type of attack.[62] Gaining access to Powershell is prized by cybercriminals "Not only are fileless attacks increasing, but PowerShell is becoming the attacker's tool of choice for these attacks. . . ."[63] Powershell attacks on a Windows system "are successful . . . because they are fileless and run from memory, preventing detection by common anti-virus applications."[64] Leveraging Powershell capabilities to infiltrate computer systems is a form of living on the land for attackers.[65] Powershell exploits are currently a concern in the memory forensic community.[66]

Live acquisition or live analysis of volatile memory evidence may be critical in investigations involving sophisticated malware.[67] Large companies and organizations that are often the target of sophisticated cyberattacks cannot simply shutdown thousands of networked computers in order to investigate the attack.[68] Traditional hard drive focused digital forensics may be ineffective in uncovering these types of attacks.[69] Shutting down a computer compromised by fileless malware will likely result in the permanent loss of the most important potential evidence about the attack. Therefore, potential evidence of malware needs to be properly analyzed or captured from a running computer.[70] Memory forensics on a live computer might also be necessary because advanced malware is often encrypted when stored but must be decrypted in memory to actually work.[71]

Malware In Volatile Memory

In general, malware needs to operate or "run" in memory in order to accomplish some type of harm.[72] If a malware program was installed in some hidden location on the hard drive, it might be relatively harmless until it is "executed" and therefore running in memory at some point.[73] However, this does not mean that a computer user has to click on or open a file to trigger malware to execute.[74]

A potential weakness of advanced malware is that it must at some point be running on a live computer. This also shows the severe limitation of traditional computer forensics focused on hard drive evidence: "If evidence of compromise is never written to a hard drive, you cannot rely on disk forensics. Memory, on the other hand, has a high potential to contain malicious code from an infection, in whole or in part, even if it's never written to disk – because it must be loaded in memory to execute."[75] Malware authors are aware of live memory forensics and may write anti-forensic capabilities into their malware to try and subvert live memory analysis.[76]

The response of a cybersecurity experts to a computer or network security compromise is commonly

referred to as "incident response." Evidence in the memory of the compromised computer is of paramount importance in these types of case.[77] Therefore, a critical part of an incident response is to preserve potential evidence in the memory of the compromised computer.

Significantly, this is also the evidence most in danger of being lost: "A memory image should be the first step taken in a suspected system compromise, as memory is the most volatile data within a system."[78] Corporate counsel are increasingly involved in cybersecurity prevention and incident response investigations and thus need some basic knowledge about the importance of preserving potential evidence in volatile computer memory.[79]

Notes

1. Jenia I. Turner, Managing Digital Discovery in Criminal Cases, 109 J. Crim. L. & Criminology 237, 239 (2019) ("Digital evidence in criminal cases is exploding. More and more crimes, from theft to drug trafficking to child pornography, are committed in cyberspace. Smartphones, digital devices, and programmable home appliances have become central to our daily lives, and the evidence they generate is increasingly used in the prosecution and defense of criminal cases."); *Foreman v. State*, No. 14-15-01005-CR, 2018 WL 4183716, at *19 (Tex. App. Aug. 31, 2018) ("Surveillance cameras inside commercial properties have become ubiquitous. Convenience stores. Doggy daycare facilities. Casinos. Retail check-out lines. Interior commercial video surveillance systems, designed to prevent internal theft, vandalism, and other forms of criminal activity from occurring on an owner's property or to catch those responsible for the activity, are everywhere.").
2. Michael R. Doucette, Virginia Prosecutors' Response to Two Models of Pre-Plea Discovery in Criminal Cases: An Empirical Comparison, 73 Wash. & Lee L. Rev. Online 415, 430 (2016) ("With modern technology, law enforcement generates far greater discoverable information. Dash-mounted camera video, body worn camera video, and jailhouse telephone audio are just a few examples of this new technology. One individual traffic stop could generate several hours of video and audio evidence.").
3. *United States v. Cyr*, No. 2:14-CR-19, 2015 WL 4773099, at *2 (D. Vt. Aug. 12, 2015) (A forensic investigator "began her investigation by making a forensic copy of the hard drive. This copy was an identical bit for bit image of the drive and enabled her to examine its contents while keeping the evidence itself pristine.").
4. Richard Boddington, Practical Digital Forensics at 92 (2016) ("Preventing any intentional or unintentional tampering of the evidence is paramount. If the evidence is not maintained in pristine condition, some inconvenient and probing challenge from the opposing legal team may well be anticipated.").
5. DFRWS 2005 Forensics Challenge "MEMORY ANALYSIS was one of the primary themes of DFRWS 2005." *http://old.dfrws.org/2005/challenge/*; Hajime Inoue, Frank Adelstein, Robert A. Joyce, Visualization in Testing a Volatile Memory Forensic Tool, 8 Digital Investigation, S42-S51 (2011) ("The area of volatile memory forensics has been rapidly growing since the 2005 DFRWS memory challenge (DFRWS, 2005)."); Harlan Carvey, Windows Forensic Analysis DVD Toolkit, at 120 (2d ed., 2018) ("With the DFRWS 2005 Memory Challenge as a catalyst, steps have been taken in an attempt to add context to the information round in RAM."); Heikki Topi, Allen Tucker, eds., Computing Handbook, Third Edition: Information Systems and Information Technology, 56-14 (2014) ("The 2005 DFRWS memory analysis challenge, has served as an early catalyst to push the development of tools for Windows memory forensics and resulted in several early projects."); Brendan Dolan-Gavitt, Forensic Analysis of the Windows Registry in Memory, 5 Digital Investigation, S26–S32, at S27 (2008 Digital Forensic Research Workshop) ("starting with the DFRWS 2005 Memory Analysis Challenge (DFRWS, 2005), a great deal of progress has been made towards cataloging the contents of physical memory on Windows systems and documenting how to make use of the information it contains. Using freely available tools, investigators can find disk encryption keys (Walters and Petroni, 2007), list processes and threads (Schuster, 2006), and detect the presence of some techniques used by malicious software such as DLL injection and hiding (Dolan-Gavitt, 2007; Walters, 2006).").
6. Andrew Case, Golden G. Richard III, Memory forensics: The path forward, 20 Digital Investigation, 23-33, 28 (2017).
7. Johannes Stuttgen and Michael Cohen, Anti-Forensic Resilient Memory Acquisition, 10 Digital Investigation, S105-S115 (proceedings of The Digital Forensic Research Conference DFRWS 2013 USA (Aug. 2013)) ("Since host-based memory forensics was first proposed, rapid advances in the analysis techniques for memory images have taken place. Modern tools are capable of extracting detailed information about system state, configuration, and anomalies. In particular, memory analysis has proven useful for the detection of rootkits and other malware infecting the host, as well as the analysis of malicious software.").
8. Fabio Pagani, Oleksii Fedorov, Davide Balzarotti, Introducing the Temporal Dimension to Memory Forensics, 22 ACM Transactions on Privacy and Security, 9:1 (March 2019) ("Kickstarted by the Digital Forensic Research Workshop (DFRWS) conference in 2005, modern memory analysis is now one of most active areas of computer forensics. . . .").
9. Kristine Amari, Techniques and Tools for Recovering and Analyzing Data from Volatile Memory, at 8 (2009) ("The analysis of any volatile memory captured by an incident responder is currently a less precise art than the analysis of a hard disk. Hard disks have a strict pre-defined structure, and analysts know where to look for certain structures and data types on a specific kind of filesystem (FAT32, for instance). Memory, on the other hand, can be allocated and de-allocated to different areas depending on what memory is already being used; for all intents and purposes it is impossible to predict what you will find in volatile memory or where it will be stored."); Shuaibur Rahman and M. N. A. Khan, Review of Live Forensic Analysis Techniques, at 379, 8 International Journal of Hybrid Information Technology, pp.379-388 (2015) ("Live analysis aims at gathering evidence from systems using different

operations and techniques related to primary memory content. Live forensic is the most challenging kind of digital forensic investigations.").

10. Nihad A. Hassan, Digital Forensics Basics: A Practical Guide Using Windows OS, at 27 (2019) ("If the suspect computer was still running, then we should consider acquiring its volatile memory (RAM) if possible. The old-school practice was to unplug the computer and then seize it in a special antistatic case. However, modern forensic practices appreciate the great importance of acquiring volatile memory while the PC is still running. RAM memory can contain a wealth of information like cryptographic keys, IM chat logs, unencrypted contents, clipboard contents, and process information, among other things.").
11. Gupta, Kedar & Nisbet, Alastair, Memory forensic data recovery utilising RAM cooling methods, at 11, In Valli, C. (Ed.). (2016), The Proceedings of 14th Australian Digital Forensics Conference, 5-6 December 2016, Edith Cowan University, Perth, Australia ("It is fairly trivial to insert a USB drive with the required software to download the contents of RAM on to an external drive for later analysis. Whilst often this is not done, the fact that RAM may contain several gigabytes of valuable forensic evidence means that evidence is lost because the forensic investigator has not considered this area to be valuable to an investigation.").
12. Daniel B. Garrie, Plugged In: Guidebook to Software and the Law § 1:16. Memory volatile or non-volatile – Volatile memory ("There are two main types of RAM: dynamic random access memory (DRAM) and static random access memory (SRAM, pronounced s-ram). . . . DRAM is a solid chip that can access any point of data stored inside without delay, allowing the processor to access data and programs very quickly. . . . In the average personal computer, the memory is in the form of DRAM."); The Sedona Conference, The Sedona Conference Glossary: E-Discovery & Digital Information Management (Fourth Edition) A Project of the Sedona Conference Working Group on Electronic Document Retention & Production (Wg1), 15 Sedona Conf. J. 305, 349 (2014) ("Random Access Memory (RAM): Hardware inside a computer that retains memory on a short-term basis and stores information while the computer is in use. It is the working memory of the computer into which the operating system, startup applications and drivers are loaded when a computer is turned on, or where a program subsequently started up is loaded, and where thereafter, these applications are executed. RAM can be read or written in any section with one instruction sequence. It helps to have more of this working space installed when running advanced operating systems and applications to increase operating efficiency. RAM content is erased each time a computer is turned off.").
13. Thomas R. McLean & Alexander B. McLean, Dependence on Cyberscribes-Issues in E-Security, 8 J. Bus. & Tech. L. 59, 108 (2013) ("One distinguishing characteristic of RAM is that it is volatile memory, meaning it loses all the content it is currently storing once the power is cut. (This is the reason word processing software prompts the user to save their work when the computer user attempts to close the program.)"); *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 519 (9th Cir. 1993) ("It is a property of RAM that when the computer is turned off, the copy of the program recorded in RAM is lost.").
14. Nihad A. Hassan, Digital Forensics Basics: A Practical Guide Using Windows OS, at 50 (2019) ("DRAM (dynamic RAM). The term 'dynamic' refers to the fact that this memory must be constantly refreshed (thousands of times per second) to retain its contents. DRAM is the main memory that we typically see installed on PCs, workstations, servers, and smartphones. A variation of DRAM is SDRAM (synchronous DRAM), a generic name that describes the different types of DRAM (DDR2, DDR3, DDR4, where DDR stands for Double Data Rate) as they are synchronized with the clock speed of the microprocessor.").
15. Michael Hale Ligh, et al., The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory, 7 (2014) ("RAM is considered *volatile memory* because it requires power for the data to remain accessible. Thus, except in the case of cold boot attacks (*https://citp.princeton.edu/research/memory*), after a PC is powered down, the volatile memory is lost. This is the main reason why the "pull the plug" incident response tactic is not recommended if you plan to preserve evidence regarding the system's current state.").
16. Todd G. Shipley & Henry R. Reeve, Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community, at 7 (2006).
17. Vassil Roussev, Digital Forensic Science: Issues, Methods, and Challenges, 62 (2016) ("Studies have clearly demonstrated that data tends to persist for a long time in volatile memory. There is a wealth of information about the run-time state of the system that can be readily extracted, even from a snapshot.").
18. Harlan Carvey, Windows Forensic Analysis DVD Toolkit, at 90 (2d ed., 2018) ("volatile data that should be collected during live-response activities is the contents of physical memory, commonly referred to as RAM.").
19. PC Magazine Encyclopedia, Definition of: physical memory ("The term physical memory is generally used to contrast main memory with virtual memory, in which the contents of RAM are temporarily transferred to storage to make room for another program.").
20. Clint Huffman, in Windows Performance Analysis Field Guide, at 199 (2014) ("Physical memory (also known as random-access memory (RAM)) is a form of very fast, but volatile data storage. RAM modules are typically measured in nanoseconds (1000− 3), and physical disks are typically measured in milliseconds (1000− 1). This makes physical memory roughly 100,000 times faster than a common physical disk. Therefore, when possible, Windows and Windows Server keep the most frequently accessed pages of memory in physical memory and rely on a disk only if needed.").
21. J. Alex Halderman, et al., Lest We Remember: Cold Boot Attacks on Encryption Keys, at 45, Proc. 17th USENIX Security Symposium (2008) (Most security experts assume that a computer's memory is erased almost immediately when it loses power, or that whatever data remains is difficult to retrieve without specialized equipment. We show that these assumptions

are incorrect. Ordinary DRAMs typically lose their contents gradually over a period of seconds, even at standard operating temperatures and even if the chips are removed from the motherboard, and data will persist for minutes or even hours if the chips are kept at low temperatures.").

22. Eric Conrad, Seth Misenar, Joshua Feldman, CISSP Study Guide, at 88 (3rd ed. 2016) ("The volatility of RAM is a subject of ongoing research. Historically, it was believed that DRAM lost integrity after loss of power. The 'cold boot' attack has shown that RAM has remanence: it may maintain integrity seconds or even minutes after power loss. This has security ramifications: encryption keys usually exist in plaintext in RAM, and may be recovered by 'cold booting' a computer off a small OS installed on DVD or USB key, and then quickly dumping the contents of memory.").
23. Felix Freiling, et al., Advances in Forensic Data Acquisition, 35 (5) IEEE Design & Test, 63 – 74, at 67 (Sept./Oct. 2018) (A Cold boot attack is "an ingenious method to acquire a memory image of a running computer by exploiting the *remanence effect* of the modern RAM technology. In contrast to common belief, memory contents do not disappear immediately after power is cut, but rather fade away gradually over time. In practice, it can take as long as 30 seconds for memory contents to fade away completely. One aspect of this effect is that low temperatures slow down the fading process, such that by cooling down RAM chips, the remanence interval can be extended from 30 seconds up to 10 minutes.").
24. Yitbarek, Salessawi Ferede, et al., Cold Boot Attacks are Still Hot: Security Analysis of Memory Scramblers in Modern Processors, at 313, 2017 IEEE International Symposium on High Performance Computer Architecture, DOI: 10.1109/HPCA.2017.10 ("in 2008, a team of researchers demonstrated that disk encryption keys could be recovered from DDR and DDR2 DRAMs by transferring memory modules from a locked machine into an attacker's machines [3]. Since charge decay in capacitors slows down significantly at lower temperatures, they cooled the DRAMs using off-the-shelf compressed air spray cans before transferring them to another machine. This technique came to be known as a *cold boot attack*.").
25. Hardik Gohel, Himanshu Upadhyay, Security Corner: Cyber Threat Analysis with Memory Forensics, 40 (11) CSI Communications: Knowledge Digest for IT Community, 17-19, at 18 (Feb. 2017) ("Everything in any type of operating system traverses random access memory, including processes and threads, rootkits and malware, IP addresses, network sockets, URLs, open files, passwords, catches, clipboards and other user generated content, encrypted keys, configurations of hardware and software and windows registry keys and event logs.").
26. Hal Pomeranz, Detecting Malware With Memory Forensics; Simson L. Garfinkel, Digital Forensics, 101 American Scientist, 375-76 (Sept.-Oct. 2013) ("Recovering files in temporary computer memory can also be illuminating for digital evidence. The RAM of a desktop, laptop, or cell phone is a mosaic of 4,096-byte blocks that variously contain running program code, remnants of programs that recently ran and have closed, portions of the operating system, fragments of what was sent and received over the network, pieces of windows displayed on the screen, the copy-and-paste buffer, and other kinds of information."); Niranjan Reddy, Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations, at 31 (2019) (RAM artifacts include: "• Running Processes – RAM will have information for all running processes that were executed by the administrator. • Passwords in clear text – On several occasions, passwords that were used over the internet are stored in clear text in the volatile memory. • Unsaved/Open files – RAM has information about the Open/Unsaved files. • Recent chat conversations – The data from messengers and chat applications can be obtained in RAM. • Network Connections – RAM also has information about the network connections of the system.").
27. Aaron Margosis and Mark E. Russinovich, Windows Sysinternals Administrator's Reference (2011).
28. Ayman Shaaban, Konstantin Sapronov, Practical Windows Forensics, at 232 (2016).
29. Harlan Carvey, Windows Forensic Analysis DVD Toolkit, at 123 (2d ed., 2018) ("the majority of the publicly available research and tools focus on processes as a source of forensic information . . . most researchers seem to be focusing on processes."); Monnappa K A, Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware, at 382 (2018) ("When you are investigating a memory image, you will mainly focus on identifying any suspicious process running on the system.").
30. Harlan Carvey, Windows Forensic Analysis DVD Toolkit, at 123 (2d ed., 2018); Grant Osbourne, Memory Forensics: Review of Acquisition and Analysis Techniques, at xiii, Australia DSTO Defence Science and Technology Organisation (Nov. 2013) ("EPROCESS An Executive Process, or EPROCESS data structure, is a Windows API data structure that represents a process.").
31. Grant Osbourne, Memory Forensics: Review of Acquisition and Analysis Techniques, at xiii, Australia DSTO Defence Science and Technology Organisation, at 5 (Nov. 2013) ("Processes are represented in memory by an EPROCESS data structure. The EPROCESS block contains many process attributes, as well as pointers to a number of related data structures. For example, a process has one or more threads represented by an ETHREAD block.").
32. Michael Hale Ligh, et al., "The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory," at 19 (2014); Steven Anson, et al., Mastering Windows Network Forensics and Investigation (2d ed. 2012) "The thread is the part of the process that actually does work. A thread, or a thread of execution, represents the part of the process that will actually execute on the processor. Each thread is allocated a small amount of memory that only it can access.").
33. Grant Osbourne, Memory Forensics: Review of Acquisition and Analysis Techniques, at xiii, Australia DSTO Defence Science and Technology Organisation, at 5 (Nov. 2013).
34. Some programs might have multiple processes running.
35. *Remijas v. Neiman Marcus Grp., LLC*, 341 F. Supp. 3d 823, 824 (N.D. Ill. 2018); Eddy Willems, Cyberdanger: Understanding and Guarding Against Cybercrime, at 1 (2019) ("Malware

(. . . an abbreviation for Malicious Software) is a collective term for all types of software that have been written with malicious intent. Viruses, worms, Trojans, spyware, and all other forms of malicious and potentially damaging software fall under the generic term 'malware.'").

36. *https://www.av-test.org/en/statistics/malware/*.
37. James Scott, Signature Based Malware Detection is Dead, at 4, Institute for Critical Infrastructure Technology (Feb. 2017) ("Signature and behavioral based anti-malware are no match for next generation adversaries who utilize mutating hashes, sophisticated obfuscation mechanisms, self-propagating malware, and intelligent malware components. It is no longer enough to detect and respond. Artificial intelligence offers the predictive quality that can give organizations a much-needed edge on their more sophisticated, less burdened, and more evasive adversaries.").
38. Arzu Gorgulu Kakisim, et al., Analysis and Evaluation of Dynamic Feature-Based Malware Detection Methods, 248, Innovative Security Solutions for Information Technology and Communications, 11th International Conference, SecITC 2018, Bucharest, Romania, November 8–9, 2018, Revised Selected Papers
39. Michael Hale Ligh, et al., The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory, 251 (2014).
40. Harlan Carvey, Windows Forensic Analysis DVD Toolkit, at 387 (2d ed. 2018) ("a rootkit is a software program that modifies the operating system so that it is capable of hiding itself and other objects from users, administrators, and even the operating system. Rootkits are used to hide processes, network connections, Registry keys, files, and the like from the operating system and, by extension, the administrator."); Rootkits, Microsoft Docs (Sept. 4, 2019) *https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/rootkits-malware* ("Malware authors use rootkits to hide malware on your device, allowing malware to persist as long as possible. A successful rootkit can potentially remain in place for years if it is undetected. During this time it will steal information and resources. . . . Rootkits intercept and change standard operating system processes. After a rootkit infects a device, you can't trust any information that device reports about itself. For example, if you were to ask a device to list all of the programs that are running, the rootkit might stealthily remove any programs it doesn't want you to know about. Rootkits are all about hiding things. They want to hide both themselves and their malicious activity on a device.").
41. Jesse D. Kornblum, Exploiting the Rootkit Paradox with Windows Memory Analysis, at 1-2, 5 International Journal of Digital Evidence (Fall 2006).
42. Ioana Vasiu & Lucian Vasiu, Riders on the Storm: An Analysis of Credit Card Fraud Cases, 20 Suffolk J. Trial & App. Advoc. 185, 203–04 (2015); David W. Opderbeck, Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry, 75 Md. L. Rev. 935, 959 (2016) ("most of the recent high profile data breach incidents that have resulted in mass tort litigation arose in the 'big box' retail context and involved the theft of consumer credit card data. A growing variety of cyber threats involve types of malware called 'RAM scrapers' that are able to capture credit card stripe data housed temporarily in the random access memory of computer systems used by retailers to process payments. This vulnerability made big box retailers who process enormous volumes of credit card transactions attractive targets for cyber criminals.").
43. *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 242 (3d Cir. 2015).
44. *Id.*
45. *In re Brinker Data Incident Litig.*, No. 3:18-CV-686-J-32MCR, 2019 WL 3502993, at *2 (M.D. Fla. Aug. 1, 2019) ("The amount of data breaches involving the theft of retail payment card information has been rising over the past several years, and '[m]ost of the massive data breaches occurring within the last several years involved malware placed on POS systems used by merchants.'").
46. Tyler (Tianqiang) Cui, An Approach to Detect Malware Call-Home Activities, at 2 (December 16, 2013), SANS Institute Reading Room ("One of the activities that malware will conduct is 'call-home', to either fetch updates and instructions from the remote Command and Control (C&C) servers, or send back stolen information.").
47. Jorg Abraham, The Implications of Silent Injection Malware on Retail Security, Infosecurity Magazine (April 26, 2018).
48. Paul Ivan, Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox, at 4, European Policy Centre (March 18, 2019) ("In May 2017, the WannaCry ransomware attack quickly spread around the world, encrypting data and demanding ransom payments in the cryptocurrency Bitcoin. The attack was estimated to have affected more than 300,000 computers across 150 countries, causing between USD 4 to 8 billion worth of damages. . . . The attack also hit the national healthcare system in the UK, which left hospitals and doctors unable to access patient data and led to the cancellation of operations and medical appointments.").
49. Avinash Singh, et al., Digital Forensic Readiness Framework for Ransomware Investigation at 95 in Digital Forensics and Cyber Crime, 10th International EAI Conference, ICDF2C (September 10-12, 2018) ("WannaCry encrypts each file with a different AES-128 key which is further encrypted with an RSA key pair and then added to the file header of each file. In order to get the decryption key, the private key of the Command and Control (C2) server is needed in order to decrypt the encrypted AES-128 decryption key. . . .").
50. Nilay R. Mistry and M. S. Dahiya, Signature based volatile memory forensics: a detection based approach for analyzing sophisticated cyber attacks, 11 International Journal of Information Technology, 583-589, at 585 (2019) ("Memory forensics helps in analyzing advanced level malwares; Ransomwares from acquired memory, malware and other important artifacts can be analyzed more thoroughly. For example, memory forensics of famous attacks like WannaCrypt, Locky revealed some artifacts related with overall behavior of the Ransomware and its encryption scripts, which were not noticed by anti-virus tools or other security solutions.").

51. *https://www.malwarebytes.com/emotet/*; Mario Trujillo, Computer Crimes, 56 Am. Crim. L. Rev. 615, 622 (2019) ("Trojan horses, or simply 'Trojans,' are computer programs with legitimate functions that also contain hidden malicious code. Like its namesake, a Trojan tricks a user into installing the seemingly innocent program on a computer system and then activates the hidden code, which may release a virus or allow an unauthorized user access to the system.").
52. Alert (TA18-201A), Emotet Malware (July 20, 2018) *https://www.us-cert.gov/ncas/alerts/TA18-201A*.
53. Emotet: Emotet is a kind of malware originally designed as a banking Trojan aimed at stealing financial data, but it's evolved to become a major threat to users everywhere, *available at* Malwarebytes *https://www.malwarebytes.com/emotet/*.
54. Steven Anson, et al., Mastering Windows Network Forensics and Investigation (2d ed. 2012) (In a hacker or intrusion investigation "hacker tools frequently run only in system memory and leave no trace on the hard disks, . . . [the examiner] now has to consider the fact that pulling the power plug may actually lose more evidence than it preserves. In such a case, touching the keyboard in order to extract and preserve evidence in RAM may be worth the cost of altering some system time stamps.") (Chapter 6 - Live-Analysis Techniques).
55. James Graham, Ryan Olson, Rick Howard, Cyber Security Essentials, 267-68 (2016) ("Attackers design some malware to run completely from RAM (i.e., memory resident codes) to avoid touching longer term storage devices such as the hard drive. Therefore, if analysts do not look for signs of intrusions in RAM, they might miss the most important, or perhaps the only, evidence that malware existed on the system.").
56. SO YOU THINK YOU'VE BEEN COMPROMISED . . ., NCCIC (National Cybersecurity and Communications Integration Center) ("The volatile memory in a system is a gold mine of forensics data, often containing information that cannot be found on the hard drive or anywhere else. Some advanced malware has even evolved to erase any sign of its presence except for the code in memory that it needs to run. For these reasons, those responding to an incident should make every effort to capture a memory image using software such as DumpIt, FTK Imager Lite, or software of similar capability.").
57. Kris Lovejoy, The Rise of Fileless Malware (September 4, 2018) ("Fileless malware is also known as 'memory-based' malware because its malicious functionality does not reside in a file on an infected host. Rather, it usually injects code into a host's random-access memory (RAM) and/or registry. . . . These attacks . . . are extremely stealthy since they don't write any new files to the disk, making the malicious code effectively invisible to antivirus programs."); Lee Neely, Endpoint Protection and Response: A SANS Survey, at 10 (2019) (In a survey of 277 IT professionals the respondents noted that in trying find artifacts to investigate compromises: "The largest gap lies in discovery of memory-resident objects where antivirus and traditional security mechanisms fail. Detecting memory objects is key for the detection of and response to file-less malware. Respondents from prior surveys also voiced concerns over lack of these artifacts, which are themselves an effective, if not strongly preferred, way to perform postinfection analysis."); Adam Kujawa, Under the Radar – The Future of Undetected Malware, at 2 (2018) (In regard to sophisticated attacks "Foremost in volume today are fileless attacks and compromises. These have had success in attacking businesses because the majority of past and present security solutions are designed to detect file-based malware. Those traditional security solutions, deployed at almost every business in the connected world, are simply not built to detect and remove malware that resides in memory rather than on the disk.").
58. Internet Security Threat Report ISTR: Living off the land and fileless attack techniques (Symantec), at 4 (July 2017) ("'Living off the land' is one clear trend in targeted cyber attacks at the moment. Attackers are increasingly making use of tools already installed on targeted computers or are running simple scripts and shellcode directly in memory. Creating less new files on the hard disk means less chance of being detected by traditional security tools and therefore minimizes the risk of an attack being blocked.").
59. Lorenz Liebler, Harald Baier, Approxis: A Fast, Robust, Lightweight and Approximate Disassembler Considered in the Field of Memory Forensics, at 158, in Matoušek, Petr, Schmiedecker, Martin. eds., Digital Forensics and Cyber Crime 9th International Conference, ICDF2C 2017, Prague, Czech Republic, October 9-11, 2017, Proceedings ("Detecting known malicious code in memory is a challenging task. This is mainly due to two reasons: first, malware authors tend to obfuscate their code by tampering it for each instance. Second, code in memory differs from persistent code because of changes performed by the memory loader (e.g., the security feature Address Space Layout Randomization (ASLR) makes it impossible to predict the final state of an executable right before run time). Hence an approach to identify malicious code within a memory forensics investigation by comparing code fragments in its untampered shape (e.g., as an image on disk) to its memory loaded representation (e.g., a module with variable code) is a non-trivial task.").
60. Getting Started with Windows PowerShell *https://docs.microsoft.com/en-us/powershell/scripting/getting-started/getting-started-with-windows-powershell?view=powershell-6*.
61. "Windows PowerShell is a task-based command-line shell and scripting language designed especially for system administration. Built on the.NET Framework, Windows PowerShell helps IT professionals and power users control and automate the administration of the Windows operating system and applications that run on Windows." *https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/powershell*.
62. Monnappa K A, Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware, at 258 (2018) ("The major reason why attackers use Powershell is that it provides access to all major operating system functions and it leaves very few traces, thereby making detection more difficult.").
63. Timothy Hoffman, PowerShell Security: Is it Enough?, SANS Institute Reading Room, at 2 (Feb. 2019).
64. *Id.* at 19.

65. Mike O'Leary, Cyber Operations: Building, Defending, and Attacking Modern Computer Networks, 2d ed., at 575 (2019) ("PowerShell has become one of the key tools in any administrator's toolbox. At the same time, attackers have also recognized the power of PowerShell and use it for their own ends. One big advantage PowerShell provides to the attacker is that they do not need to upload binaries to the target - binaries that could be detected and traced. An attacker that can live off the land and use only the tools already present on the system is much more difficult to detect.").
66. Andrew Case, Golden G. Richard III, Memory forensics: The path forward, 20 Digital Investigation, 23-33, 29 (2017) ("Memory forensics is currently lacking in two key areas for Windows systems. The first is the ability to detect Powershell activity in a post mortem investigation. . . . Current capabilities against Powershell generally rely on string searching or looking for side-effects of the actions taken by Powershell scripts and not the actual Powershell activity itself.").
67. Cristiano Giuffrida, Sébastien Bardin, Gregory Blanc, eds., Detection of Intrusions and Malware, and Vulnerability Assessment, at 47, Proceedings of the 15th International Conference, DIMVA 2018 (June 28-29, 2018) ("Recently cyber security professionals came up with a new term for targeted attacks employing non-persistent in-memory malware and named them as Advanced Volatile Threats, because there is no easy way to detect them other than analyzing volatile memory. In order to detect fileless malware and also malware that hides its presence on the system by using advanced malware stealth techniques such as hooking, injection, hallowing, etc., memory analysis is a must and needed to be conducted along with dynamic analysis."); Gerard Johansen, Digital Forensics and Incident Response, at 76 (2017) ("One of the most critical pieces of volatile evidence is the memory currently running on the system. When investigating such incidents as malware infections, the memory in a live system is of critical importance. Malware leaves a number of key pieces of evidence within the memory of a system and, if lost, can leave the incident response analyst with little or no avenue to investigate.").
68. Peter Kieseberg, et al., Real-Time Forensics Through Endpoint Visibility, at 19, in Matoušek, Petr, Schmiedecker, Martin. eds., Digital Forensics and Cyber Crime 9th International Conference, ICDF2C 2017, Prague, Czech Republic, October 9-11, 2017, Proceedings ("Large companies such as Google, Facebook and Mozilla are challenged with the downsides of those standardized approaches. Like many other companies, they experienced several incidents, however they suffer from the problem of scales, having to investigate on thousands and thousands of computers. Relying on the established forensic approach and turning every computer off, making a 1:1 hard drive copy and so forth, is not only unfeasible in reality, but would cost millions of Dollars every hour. Thus the three mentioned companies are developing solutions called *real-time forensic tools*, namely Google's *GRR Rapid Response (GRR)*, Facebooks *osquery* and Mozillas *InvestiGator (MIG)*.").
69. Michael Hale Ligh, et al., The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory, Introduction (2014) ("Although inspection of hard disks and network packet captures can yield compelling evidence, it is often the contents of RAM that enables the full reconstruction of events and provides the necessary puzzle pieces for determining what happened before, during, and after an infection by malware or an intrusion by advanced threat actors.")
70. Cameron H. Malin, Eoghan Casey, James M. Aquilina, Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides (2013) ("Investigations involving malicious code rely heavily on forensic preservation of volatile data. Because operating a suspect computer usually changes the system, care must be taken to minimize the changes made to the system; collect the most volatile data first (a.k.a. Order of Volatility, which is described in detail in *RFC 3227: Guidelines for Evidence Collection and Archiving*); and thoroughly document all action taken.").
71. Harlan Carvey, Windows Forensic Analysis DVD Toolkit, at 90 (2d ed., 2018) ("Malware analysts will look to memory in dealing with encrypted or obfuscated malware, because when the malware is launched, it will be decrypted in memory. More and more, malware is obfuscated in such a way that static, offline analysis is extremely difficult at best.").
72. Jiageng Chen, Vincenzo Piuri, Chunhua Su, Moti Yung, Network and System Security: 10th International Conference, NSS 2016, Taipei, Taiwan, Proceedings, at 202 (September 28-30, 2016) ("to operate its malicious functionality, a malware must reveal its true features during run-time.").
73. Ganapathi, Padmavathi, Shanmugapriya, D., Handbook of Research on Machine and Deep Learning Applications for Cyber Security, at 109 (2019) ("Virus is a category of malware that, when executed, tries to replicate itself into other executable code, when it succeeds, the code is said to be infected. At the point when the tainted code is executed, the infection likewise executes."); Siegfried Rasthofer, et al., Making Malory Behave Maliciously: Targeted Fuzzing of Android Execution Environments, at 300, 2017 IEEE/ACM 39th International Conference on Software Engineering ("ICSE") (On Android mobile operating systems "To avoid being detected as malware through automated or manual analysis, many malware apps exhibit their maliciousness only when being executed in a particular environment. For example, some apps check whether they are running in an emulator or another analysis environment, and behave benignly in these cases. Other malware apps target specific countries and remain harmless unless the SIM card in the victim's phone is registered in one of the target countries. Yet another kind of malware targets devices with a specific app installed, such as a vulnerable banking app.").
74. Eddy Willems, Cyberdanger: Understanding and Guarding Against Cybercrime, at 117 (2019) ("Myth 7: If I do not open an Infected File, It Can't Do Any Harm . . . The times are long gone when a file only got to be opened (or executed) if the user chose to open it. The fact is, a file can be opened or executed without any intervention by the user.").
75. Michael Hale Ligh, et al., The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory, xviii (2014).

76. *Id*. at 819 ("malware can subvert live forensics tools, . . . Because system administrators and security tools often rely on the live system APIs to find malware infections, attackers make a concerted effort to filter data out of the operating system's reporting channels. This makes it difficult to detect advanced malware on a running system.").
77. Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, U.S. Department of Health and Human Services & Healthcare & Public Health Sector Coordinating Councils, at 18 (December 28, 2018) ("If you discover that your computer has been infected, immediately disconnect from the network and notify your IT security team. Do not power off or shut down the computer or server, in case a volatile (RAM) memory image needs to be collected for forensics and incident response investigations.").
78. Wylie Shanks, Enhancing incident response through forensic, memory analysis and malware sandboxing techniques, at 8 (2014) *available at https://www.sans.org/reading-room/whitepapers/incident/enhancing-incident-response-forensic-memory-analysis-malware-sandboxing-techniques-34540*.
79. Jennifer Martin, Mitigating Litigation Risk: The Essential Role of Legal Counsel in Cybersecurity Incident Response, 72 Consumer Fin. L.Q. Rep. 285, 289 (2018) ("Employees and users should be told what to do and what *not* to do if they suspect or experience a cybersecurity issue. Specifically, users should not attempt to 'investigate' themselves, or turn-off or wipe a computer unless explicitly directed to do so by the information security team. Doing so can destroy or modify critical digital evidence, including volatile evidence in memory.").

Current Developments

By Steven A. Meyerowitz

Administrative Actions

Interior Secretary Grounds Agency's Drone Fleet for Non-Emergency Operations

U.S. Secretary of the Interior David Bernhardt has signed Secretary's Order 3379, ordering the temporary cessation of non-emergency unmanned aircraft systems fleet operations.

Agency spokesperson Carol Danko said, "Drones are important to critical Department of the Interior missions, such as combating wildfires and conducting life-saving search and rescue operations; however, we must ensure that the technology used for these operations is such that it will not compromise our national security interests. After an ongoing review of Interior's drone program, Secretary Bernhardt issued a Secretary's Order today, affirming the temporary cessation of non-emergency drones while we ensure that cybersecurity, technology, and domestic production concerns are adequately addressed. Drone use for non-emergency operations will remain grounded while the Department of the Interior reviews the possibility of threats and ensures a secure, reliable and consistent drone policy that advances our mission while keeping America safe. Drone operations will continue to be allowed in approved situations for emergency purposes, such as fighting wildfires, search and rescue, and dealing with natural disasters that may threaten life or property."

In Congress

Bill Granting CISA Subpoena Authority Passes House Committee on Homeland Security

The House Committee on Homeland Security has favorably reported H.R. 5680, the Cybersecurity Vulnerability Identification and Notification Act. The bill was introduced by Congressman Jim Langevin (D-RI), a senior member of the committee.

H.R. 5680 amends the Homeland Security Act of 2002, granting the Cybersecurity and Infrastructure Security Agency ("CISA") administrative subpoena authority to help identify and notify critical infrastructure entities of cybersecurity vulnerabilities on their systems.

According to Congressman Langevin, the bill aims to address instances in which the CISA identifies a vulnerable system but is limited in its response because it cannot identify and engage with the system's owner. Under current policy, telecommunications companies that may have relevant subscriber information that could make it easier to identify the subscriber assigned an IP address, are prohibited under the Electronic Communications Privacy Act from disclosing it to the U.S. government, absent of a compulsory legal process.

Under the bill, the director of the CISA only would be able to issue a subpoena when the agency knows of a specific cybersecurity risk to an entity but is unable to determine who the entity is. The subpoena authority only applies to basic categories of subscriber information such as name, address, and telephone number. The legislation makes clear that such data are only to be used for notification about a risk, not for surveillance or investigation purposes. After being contacted by CISA, an entity would choose whether to request further assistance or not.

H.R. 5680 is cosponsored by Representatives John Katko (R-NY), Bennie Thompson (D-MS), Cedric Richmond (D-LA), Sheila Jackson Lee (D-TX), and John Ratcliffe (R-TX). Similar legislation was introduced in the Senate by Senators Ron Johnson (R-WI) and Maggie Hassan (D-NH). The bill will now be forwarded to the full House for consideration.

The full text of H.R. 5680 is available at *https://homeland.house.gov/imo/media/doc/BILLS-116hr5680ih.pdf*.

Steven A. Meyerowitz, a Harvard Law School graduate, is the founder and president of Meyerowitz Communications Inc., a marketing communications consulting company. Mr. Meyerowitz is co-executive editor of *The Computer & Internet Lawyer* and editor of the *Intellectual Property & Technology Law Journal*, *Employee Benefit Plan Review*, and *Employee Relations Law Journal*, all published by Wolters Kluwer. He may be contacted at *smeyerowitz@meyerowitzcommunications.com*.

Legislation Seeks to Establish Cybersecurity Coordinator in Every State

U.S. Senators Maggie Hassan (D-NH), John Cornyn (R-TX), Rob Portman (R-OH), and Gary Peters (D-MI) have introduced a bipartisan bill to require the U.S. Department of Homeland Security to establish a Cybersecurity State Coordinator program. Under the bill, each state would have its own federally funded cybersecurity coordinator, who would be responsible for helping to prevent and respond to cybersecurity threats by working with federal, state, and local governments as well as schools, hospitals, and other entities.

The Cybersecurity State Coordinator program would be housed in the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. The coordinators would:

- Improve coordination within federal entities and between federal and non-federal entities, including state and local governments and other organizations;
- Support preparation, response, and remediation efforts relating to cybersecurity risks and incidents, including ransomware;
- Facilitate the sharing of cyber threat information; and
- Raise awareness of financial, technical, and operational resources that the federal government offers to non-federal entities to help prevent cyber threats.

The text of the legislation is available at *https://www.hassan.senate.gov/imo/media/doc/CyberStateCoordinatorAct.pdf*.

Sorry, Wrong Number

Scammers Are Spoofing FBI Phone Number in Government Impersonation Fraud

The FBI has seen a recent increase in phone calls that spoof its phone number as part of a Social Security scam. The callers often will "spoof," or fake, the FBI Headquarters' phone number, 202-324-3000, so the call appears to be coming from the FBI on the recipient's caller ID.

In this scam, fraudulent callers posing as an FBI agent inform the victim that their Social Security number has been suspended. The scammer provides a fake name and badge number to trick the victim into believing they are an FBI agent. The scammer tells the victim that in order to get their Social Security number reinstated, they must purchase gift card(s), put money on the card(s), and call the scammer back and provide the gift card number(s). Instead of providing any additional information on the victims' Social Security number, the scammer will hang up.

The FBI has pointed out that these calls are fraudulent and that any legitimate law enforcement officer will not demand cash or gift cards from a member of the public. The FBI defines this type of scam as government impersonation fraud, in which criminals impersonate government officials in an attempt to collect money. The criminals often threaten to extort victims with physical or financial harm to obtain personally identifiable information. Scammers are becoming more sophisticated and organized in their approach, are technologically savvy, and often target young persons and the elderly.

According to the Internet Crime Complaint Center ("IC3"), 13,873 people reported being victims of government impersonation scams in 2019, with losses totaling more than $124 million.

Justice Department Alleges Telecom Carriers Facilitated Hundreds of Millions of Fraudulent Robocalls to American Consumers

The U.S. Department of Justice has filed civil actions for temporary restraining orders today in two cases against five companies and three individuals allegedly responsible for carrying hundreds of millions of fraudulent robocalls to American consumers.

The Justice Department alleged that the companies were warned numerous times that they were carrying fraudulent robocalls – including government- and business-imposter calls – and yet continued to carry those calls and facilitate foreign-based fraud schemes targeting Americans. The calls, most of which originated in India, led to massive financial losses to elderly and vulnerable victims across the nation, according to the department.

The two cases contained similar allegations. The defendants in one case were Ecommerce National LLC d/b/a TollFreeDeals.com; SIP Retail d/b/a sipretail.com; and their owner/operators, Nicholas Palumbo and Natasha Palumbo of Scottsdale, Arizona. The defendants in the other case included Global Voicecom Inc., Global Telecommunication Services Inc., KAT Telecom Inc., aka IP Dish, and their owner/operator, Jon Kahen, of Great Neck, New York.

The government alleged that the defendants operated voice over internet protocol ("VoIP") carriers, which use an internet connection rather than traditional copper phone lines to carry telephone calls. Numerous foreign-based criminal

organizations are alleged to have used the defendants' VoIP carrier services to pass fraudulent government- and business-imposter fraud robocalls to American victims. The complaints specifically alleged that defendants served as "gateway carriers," making them the entry point for foreign-initiated calls into the U.S. telecommunications system and that they carried astronomical numbers of robocalls.

For example, the complaint against the owners/operators of Ecommerce National d/b/a TollFreeDeals.com alleged that the defendants carried 720 million calls during a sample 23-day period, and that more than 425 million of those calls lasted less than one second, indicating that they were robocalls. The complaint further alleged that many of the 720 million calls were fraudulent and used spoofed (that is, fake) caller ID numbers. According to the authorities, the calls facilitated by the defendants falsely threatened victims with a variety of catastrophic government actions, including termination of social security benefits, imminent arrest for alleged tax fraud and deportation for supposed failure to fill out immigration forms correctly.

According to allegations in both complaints, the defendants ignored repeated red flags and warnings about the fraudulent and unlawful nature of the calls they were carrying.

Election Security

FBI Announces New Policy for Notifying State and Local Election Officials of Cyber Intrusions Affecting Election Infrastructure

The Federal Bureau of Investigation ("FBI") has announced a new internal policy to clarify and guide the timely federal notification of appropriate state and local officials of cyber intrusions affecting election infrastructure.

Cyber intrusions affecting election infrastructure have the potential to cause significant negative impacts on the integrity of elections. Understanding that mitigation of such incidents often hinges on timely notification, the FBI has established a new internal policy outlining how the FBI will notify state and local officials responsible for administering election infrastructure of cyber activity targeting their infrastructure.

The FBI's new policy recognizes the necessity of notifying responsible state and local officials of credible cyber threats to election infrastructure. Each state has a designated person to serve as its chief state election official with ultimate authority over elections held in the state, which often includes certifying election results. However, most election infrastructure is owned and operated by local governments. Likewise, the local election process is overseen by local election officials. The FBI's interactions regarding election security matters must respect both state and local authorities. Thus, the FBI's new policy mandates the notification of a chief state election official and local election officials of cyber threats to local election infrastructure.

The new policy is informed by existing FBI policies surrounding cyber incident notification thresholds and cyber victim notification in general. The new policy, however, provides updated and additional guidance on the timely dissemination of notifications and/or threat reporting; the protection of victim information and disclosures; and coordination between FBI and other agencies in regard to election security for maximum impact. Decisions surrounding notification continue to be dependent on the nature and breadth of an incident and the nature of the infrastructure impacted.

The FBI said in a statement that it was the intent of the FBI for this new policy to result in increased collaboration between all levels of government for the integrity and security of U.S. elections.

Data Privacy

Government Seizes WeLeakInfo.com Domain Name

The Federal Bureau of Investigation and the U.S. Department of Justice have seized the internet domain name weleakinfo.com.

The government asserted that the website had claimed to provide its users a search engine to review and obtain the personal information illegally obtained in over 10,000 data breaches containing over 12 billion indexed records – including, for example, names, email addresses, usernames, phone numbers, and passwords for online accounts. According to the authorities, the website sold subscriptions so that any user could access the results of these data breaches, with subscriptions providing unlimited searches and access during the subscription period (one day, one week, one month, or three months).

With execution of the warrant, the seized domain name – weleakinfo.com – is now in the custody of the federal government, effectively suspending the website's operation. Visitors to the site will now find a seizure banner that notifies them that the domain name has been seized by federal authorities. The U.S. District Court for the District of Columbia issued the seizure warrant.

Any persons having information concerning weleakinfo.

com or its owners and operators are encouraged to provide that information by filing a complaint (referencing #weleakinfo in the "Description of Incident" field) with the FBI's Internet Crime Complaint Center (IC3) at *https://www.ic3.gov/complaint/default.aspx*.

FTC Action

FTC Warns 19 VoIP Service Providers That 'Assisting and Facilitating' Illegal Telemarketing or Robocalling Is Against the Law

Federal Trade Commission (FTC) staff have sent letters to 19 voice over internet protocol (VoIP) service providers warning them that "assisting and facilitating" illegal telemarketing or robocalling is against the law.

The letters warn the VoIP service providers that the FTC may take legal action against them if they assist a seller or telemarketer that they know, or that they consciously avoid knowing, is violating the agency's Telemarketing Sales Rule (TSR).

The FTC did not disclose the names of the companies or individuals to whom it sent the warnings.

The letters noted several types of conduct that may violate the TSR, including:

- Making a false or misleading statement to induce a consumer to buy something or contribute to a charity;
- Misrepresenting a seller or telemarketer's affiliation with any government agency;
- Transmitting false or deceptive caller ID numbers;
- Initiating pre-recorded telemarketing robocalls, unless the seller has express written permission to call; and
- Initiating telemarketing calls to consumers whose phone numbers are on the National Do Not Call Registry, with certain exceptions.

The letters stressed that combatting illegal telemarketing is a top priority of the FTC, with a special emphasis on stopping illegal robocalls.

FTC Finalizes Settlements with Four Companies Related to Privacy Shield Allegations

The Federal Trade Commission (FTC) has finalized settlements with four companies over allegations they made false claims in connection with the EU–U.S. Privacy Shield framework, which enables companies to transfer consumer data legally from European Union countries to the United States.

In separate actions, the FTC alleged that Click Labs, Inc., and Incentive Services, Inc., falsely claimed to participate in the EU–U.S. Privacy Shield framework and the Swiss-U.S. Privacy Shield framework, which establishes a process for companies to transfer consumer data in compliance with Swiss law.

The FTC also alleged that Global Data Vault, LLC, and TDARX, Inc., continued to claim participation in EU–U.S. Privacy Shield after allowing their certifications to lapse. According to the FTC, they also substantively violated the Privacy Shield principles by failing to verify annually that statements about their Privacy Shield practices were accurate and failing to affirm that they would continue to apply Privacy Shield protections to personal information collected while participating in the program.

Under the settlements, all four companies are prohibited from misrepresenting their participation in the EU–U.S. Privacy Shield framework, as well as any other privacy or data security program sponsored by any government or any self-regulatory or standard-setting organization. As part of their settlements, Global Data Vault and TDARX also are required either to continue to apply the Privacy Shield protections to personal information they collected while participating in the program, or to return or delete the information.

Wolters Kluwer

Wolters Kluwer
The Computer & Internet Lawyer
Distribution Center
7201 McKinney Circle
Frederick, MD 21704

TIMELY REPORT
Please Expedite

April/10041447-0400