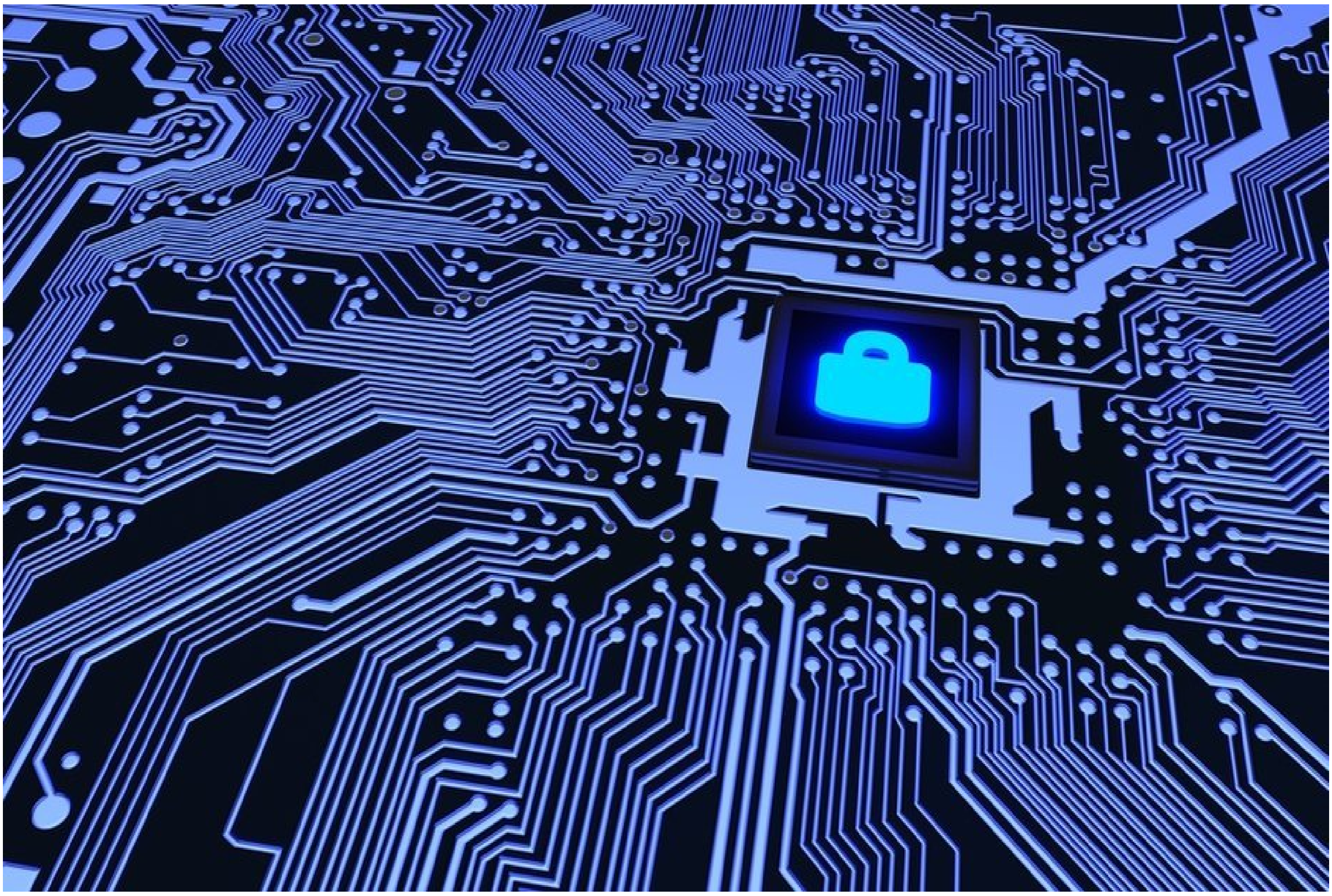
gt (/)

SECURITY
(/security)

Tips for Guarding Against Untraceable, 'Fileless' Cyberattacks

With public software increasingly less vulnerable, bad actors are utilizing legitimate tools already on users' systems — and so-called 'fileless' attack techniques that leave no trace.

BY THEO DOUGLAS (HTTP://WWW.GOVTECH.COM/AUTHORS/THEO-DOUGLAS.HTML) / JULY 24, 2017



SHUTTERSTOCK

A cybercrime trend with alarming implications for public agencies remains popular as the year wears on; called "living off the land," the technique is drawing increased interest from attackers looking to further reduce their profiles, a new white paper has found.

“Living off the land” techniques use tools already installed on users’ systems to access sensitive data — and are a “clear trend in targeted cyber attacks,” according to *Living Off the Land and Fileless Attack Techniques* (https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-living-off-the-land-and-fileless-attack-techniques-en.pdf), a special Internet Security Threat Report released July 12 by cybersecurity company Symantec.

Accompanying that trend, authors wrote, is a “growing interest” in four types of “fileless infection techniques:"

- **Memory-only threats** run in a computer’s memory, with nothing written onto a file or disk; machines disinfect themselves when they reboot or restart, leaving no trace.
- **Fileless persistence** ensures attacks begin anew even after a restart and disinfect, with the most popular strategy imbedding malicious script data inside a computer’s registry.
- **Dual-use tools** are clean tools used legitimately by a computer’s owner, but can be co-opted by hackers to their own benefit or downloaded afterward.
- **Non-Portable Executable** (non-PE) file attacks are attacks not using binary executable (EXE) or dynamic-link library (DLL) files. Visual Basic Script, JavaScript and PowerShell are the three basic examples commonly seen. Each can complete the same tasks but look different doing so, thereby avoiding detection.

Candid Wueest, a principal threat researcher and main author of the report, told *Government Technology* that hackers continue to evolve their strategies to avoid being found out because vulnerabilities in public software are getting harder to find.

Two recent exceptions, he noted, are the WannaCry and Petya ransomware attacks, which exploited a flaw in Server Message Block, used in instances including file sharing to remote Microsoft Windows services. But simplistic, hard-to-spot strategies are becoming more common.

“The attackers are falling back to proven methods, which are usually simple, but with a little bit of social engineering and clever wording, they are nevertheless still successful," Wueest told *Government Technology*. "Why would they spend a lot of money or resources to find exploits if they can simply do an invoice attached to an email and have someone deliberately infect themselves?”

In Missouri, state CISO Michael Roling told *Government Technology* that officials have “seen an uptick” in these types of activity and watched hackers’ tactics change in recent years, demonstrating that mere signature-based malware detection is just not good enough anymore.

“We see a mix of various attack methods, and oftentimes there may be more than one technique used. The art of deception — these attackers, they’ve crafted that,” Roling said, indicating that officials have seen malware over the years that capitalizes on “vulnerable plug-ins and extensions.”

This isn’t the first time fileless infection techniques have risen in popularity, Symantec authors wrote. The Code Red worm, which emerged in 2001, existed in memory and wrote no files to disk. In 2014, these types of attacks spiked again, driven by fileless persistence methods from threats like Trojan.Poweliks, which lives in a computer’s registry.

Wueest said Symantec expects the popularity of fileless techniques to continue through this year and likely 2018 as well, potentially tapering off as new security mitigation tools, services and software are created.

A lessening should take “at least two years” for public government agencies, he said, because their adaptation cycles tend to be “not too quick” and funding is often tight.

On average, Wueest said, state and local government agencies tend to be “less prepared” for these types of attacks because they may not have their own Internet security operations centers with teams available around the clock.

Attacks involving dual-use tools may hit a particularly sensitive nerve by flipping agencies’ tools to a hacker’s benefit — but the most popular incursions center on non-PE files, Wueest said, noting that some groups spam out hundreds of thousands such emails daily.

Efforts to block them are improving, he said, but both are likely to be commonplace for some time.

“These two will be the main thing where we see a drastic rise in usage from all kinds of groups of cybercriminals, but also targeted attack groups. For all of them it makes sense, because they are so versatile and also so powerful to use,” Wueest said.

Attacks often begin through spear phishing, an email spoof targeting a company or individual, the threat researcher said. Public agencies are particularly at risk here because in many cases they regularly deal, and are accustomed to interacting, with new customers via email.

Best practices, however, can go a long way toward reducing that risk. Wueest recommended agencies review privileges carefully to ensure staffers have administrator rights only if it's absolutely essential. Similarly, he said networks and servers should also be segregated to restrict access.

Jerry Driessen, CIO of Hennepin County, Minn., echoed those recommendations; he emphasized that firewalls need to be strong, and network architecture and design need to be configured to keep agencies secure as Internet of Things (IoT) devices increasingly expand their reach.

"These types of intrusions need to be dealt with through active monitoring and your architectural design, especially in the context of IoT," Driessen told *Government Technology*, noting that agencies need to be vigilant because devices ranging from soda vending machines to stovetops at incarceration facilities are now capable of being part of IoT — and may themselves be easily breached.

"I would also say that contracting plays a role because of how you buy some of this stuff. Ensuring that it's not predisposed to malware coming across is critical," Driessen added.

Missouri's CISO said his state has invested in other technology and processes over the past five years to identify newer forms of attacks. Fundamental protections, Roling said, include good patch and access management, and improving end-user awareness.

More generally, Roling added, an investment in one or more of three areas is crucial if agencies hope to fight these more invisible threats.

"There is an investment to be made in either people, technology or getting the word out," Roling said. "Helping them understand the criticality of what we're faced against is absolutely vital."

Theo Douglas (http://www.govtech.com/authors/Theo-Douglas.html) Staff Writer

Theo Douglas is a staff writer for *Government Technology*. His reporting experience includes covering municipal, county and state governments, business and breaking news. He has a Bachelor's degree in Newspaper Journalism and a Master's in History, both from California State University, Long Beach.

RELATED

Petya: Another Ransomware Attack Sweeping the Globe (http://www.govtech.com/security/Petya-Another-Ransomware-Attack-Sweeping-the-Globe.html)

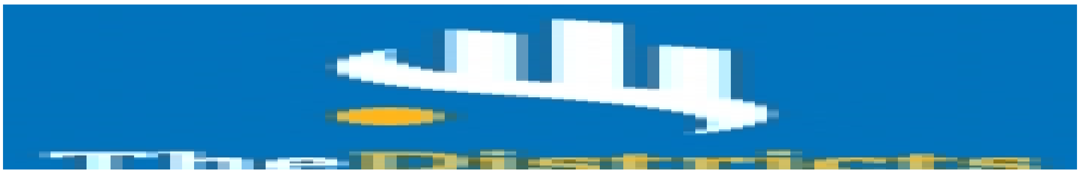
‘NotPetya’ Ransomware Attack Shows Corporate Social Responsibility Should Include Cybersecurity (http://www.govtech.com/security/NotPetya-Ransomware-Attack-Shows-Corporate-Social-Responsibility-Should-Include-Cybersecurity.html)

DISCUSS

MORE FROM SECURITY (HTTP://WWW.GOVTECH.COM/SECURITY)

NEW ON THE PODCAST

The Districts Podcast: Detroit and Houston or Bust (http://www.govtech.com/districts/podcasts/The-Districts-Podcast-Detroit-and-Houston-or-Bust.html)



APPLE PODCASTS

(https://itunes.apple.com/us/podcast/id1250965534)

STITCHER™

(http://www.stitcher.com/podcast/erepublic/the-districts)

FEATURED RESOURCES

PRESENTED BY

City of Fort Worth Integrates eProcurement and ERP (http://www.govtech.com/library/papers/The-City-of-Fort-Worth-Establishes-New-Industry-Standard-with-Integration-of-eProcurement-45843.html?promo_code=gt_paper_web_channel)

Public Procurement for the Postmodern ERP Era (http://www.govtech.com/library/papers/Public-Procurement-for-the-Postmodern-ERP-Era-46758.html?promo_code=gt_paper_web_channel)

Modernizing Public Sector Procurement (http://www.govtech.com/library/papers/Modernizing-Public-Sector-Procurement-44507.html?promo_code=gt_paper_web_channel)

Cloud Services Jumpstart Procurement Modernization (http://www.govtech.com/library/papers/Cloud-Services-Jumpstart-Procurement-Modernization-49554.html?promo_code=gt_paper_web_channel)

Tweets by @PeriscopeHldgs

Periscope Holdings Retweeted

Operational Services
@Mass_OSD

Diverse biz owners: Register to attend next week's Supplier Diversity Networking Event at @Northeastern: ow.ly/tGe530evp61 [PIC]

Annual

Supplier Diversity Networking Event

Small and diverse business owners: network with procurement professionals from colleges, universities, cultural organizations, hospitals, and local and state government!

Embed View on Twitter