# Weathering the CYBER STORM

As cybersecurity challenges evolve, so do agencies' efforts to find new ways to protect their systems

GCN Staff

**THERE'S NO ONE-AND-DONE** fix for cybersecurity. The environment evolves with ever-changing types of attacks and vulnerabilities, requiring government agencies to remain alert and proactive. But that can be challenging given the speed at which new technologies introduce risks and solutions alike.

Federal civilian agencies reported a combined 35,277 security incidents in 2017, up from 30,899 in 2016. One reason for the increase is the proliferation of new attack vectors. Take cryptocurrency mining and botnets, for instance.

Coinhive is designed to enable website owners to make money without using ads, and it is fast becoming a tool of choice for malware authors who hide it in Chrome extensions and hacked sites, according to the MIT Technology Review. Researchers say cryptocurrency-mining botnets could earn hackers $30,000 a month or even as much as $100 million a year. Crypto-mining malware affected 22 percent of organizations worldwide in May, up from 16 percent the month before.

Another emerging problem is fileless malware that can bypass antivirus protections. Last October, researchers discovered a new version of DNS Messenger that "masquerades as the Securities and Exchange Commission and hosts malware on compromised government servers," according to ZDNet. The attack sends an email message that looks like it's from an SEC system, but users who download an official-looking attachment kick off a series of infections.

## How the government is responding

The need for cybersecurity techniques that can address these new – and growing – problems is not lost on government officials. Agencies that set the tone for cybersecurity governmentwide are updating defensive programs and proactively deploying innovative responses.

For example, the Department of Homeland Security's Continuous Diagnostics and Mitigation program is moving into the third of its four phases. After determining what is on the network (Phase 1) and who is on the network (Phase 2), agencies are now focusing on what's happening on the network. DHS has started making awards under CDM's Dynamic and Evolving Federal Enterprise Network Defense set of task orders, which offer agencies increased procurement flexibility and enhanced support for cloud and mobile cybersecurity, among other improvements.

But IT managers know that despite their best efforts, the risk of a successful attack always looms. "Government agencies should be prepared to face new, self-propagating, network-based threats in 2018," Cisco's latest Annual Cybersecurity Report states.

Accordingly, every other year DHS runs the Cyber Storm drill so participants can practice collaborating on the response to a simulated cyber incident. More than 1,000 people worldwide took part in the most recent drill in April, which aimed to strengthen "cybersecurity preparedness and response capabilities by exercising policies, processes and procedures for identifying and responding to a multi-sector cyberattack targeting critical infrastructure."

In addition to governmentwide initiatives to bolster cybersecurity, agencies are taking matters into their own hands. The IRS issued a request for information in June seeking industry examples of a platform based on artificial intelligence and machine learning that could identify and mitigate insider threats. Officials said the solution should automatically and continually learn to improve accuracy, identify previously unknown threats and support the use of near-real-time data sources.

Blockchain is another technology that many government agencies are considering. Created as a digital ledger for recording cryptocurrency transactions, blockchain "addresses the fundamental flaws of security by taking away the human factor from the equation, which is usually the weakest link," a Forbes article states.

In addition, the Intelligence Advanced Research Projects Activity is developing a multiphase project that will reduce the exploitation of legacy and cloud-based vulnerabilities by focusing on users' roles rather than their identities. Each role in the Virtuous User Environment will have its own set of protective measures separate from the user's other roles.

### Empowering agencies to strengthen security

Agencies have long known that cybersecurity cannot rely on technology alone. Since 2010, the Government Accountability Office has issued about 3,000 recommendations to federal agencies on ways to improve information security programs and controls. (As of July, about 1,000 still needed to be implemented.) They include calls for an expanded cyber workforce through better recruitment and training and the use of metrics to evaluate the effectiveness of programs such as the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

It is also becoming apparent that compliance with government policies is not enough. Agencies must adopt a more complex, strategic approach to cybersecurity. The public sector far outnumbers other sectors in the number of cyber incidents — nearly 23,000, according to Verizon's 2018 Data Breach Investigations Report. That's compared to just over 1,000 for the second most-affected sector.

Procurement is another area that needs to evolve. The typically lengthy process agencies must follow does not work in the fast-paced cybersecurity world. A proposed rule published in the Federal Register in June seeks to amend the Federal Acquisition Regulation to expand special emergency procurement authorities for buying supplies or services that help agencies defend against or recover from cyberattacks.

Many agencies would like to speed procurement in general. Last year, the Defense Information Systems Agency received "other transaction authority" so it can operate outside standard procurement procedures, and the General Services Administration is studying how blockchain could help automate the FASt Lane process for IT Schedule 70 contracts.

The need for agencies to strengthen cybersecurity is not new. In fact, GAO first designated information security as a governmentwide high-risk area in 1997. In its July 2018 "High-Risk Series" report, GAO identified four major challenges and 10 critical actions to address them. The first challenge is establishing a comprehensive cybersecurity strategy and performing effective oversight.

There are efforts underway to update cybersecurity policies. Legislation introduced in July, for example, would make CDM a law and empower DHS to modernize the program. When such efforts are combined with government and industry innovations, agencies will have a solid yet adaptable foundation on which to grow their cybersecurity approaches in a continually changing environment. ■

## NEW SECURITY CHALLENGES BY THE NUMBERS

**4.2K**

**4,200 websites, including some run by the U.S. government, were hijacked in February to secretly mine cryptocurrency via visitors' computers and smartphones.**

**34 percent of cyber incidents in the public sector originate within the agency.**

**34%**

**71**

**71 of 96 federal agencies lack fundamental cybersecurity policies or have significant gaps in their cybersecurity programs.**

**31 percent of the cyber incidents reported to the U.S. Computer Emergency Readiness Team used a threat vector categorized as "other," which includes avenues of attack that are as yet unidentified.**

**31%**

**50%**

**50 percent of global web traffic was encrypted as of October 2017, up 12 points from the year before.**

Sources: Cisco, Government Accountability Office, Newsweek, Office of Management and Budget, Verizon