MSP'S GUIDE TO

3 Game-Changing Problems in Security

LEOLINTANG/SHUTTERSTOCK.COM

So far 2017 has been a typical year in security—in other words, it brought brand-new categories of thorny security problems that MSPs will tangle with for years to come.

By Scott Bekker

E**very year**, managed services providers (MSPs) can depend on one thing: There will be a few new types of threats to add to the list of security problems they already worry about on behalf of their customers.

So far in 2017, white hat researchers, bad actors and, apparently, nation states have come up with three major net new problems that promise to nag at MSPs over the years to come. They involve the previously rock-solid WPA2 wireless standard, a category of undersecured Office 365 accounts and malware derived from nation-state attack tools.

KRACK WHACKS WPA2

A long-standing pillar of modern computer security sustained major damage in October when researchers revealed a serious weakness in WPA2, the gold-standard protocol for protecting wireless networks.

The Belgian researcher who discovered the weakness, Mathy Vanhoef of KU Leuven, dubbed the new category of attacks "KRACK" for "key reinstallation attacks."

KRACK exploits a flaw in the way a client joins a WPA2-protected network, a procedure known as the four-way handshake. Critically, Vanhoef noted that the flaw exists in properly configured wireless networks. "The weaknesses are in the Wi-Fi standard itself, and not in individual products or implementations. Therefore, any correct implementation of WPA2 is likely affected," Vanhoef wrote on a Web site created to explain the vulnerability, krackattacks.com.

By manipulating and replaying cryptographic handshake messages, KRACK tricks the victim system into reinstalling keys that are already in use, Vanhoef wrote. While the attack doesn't reveal the wireless network password, it does allow some to all of the network traffic to be visible to an attacker, depending on the encryption protocol in use.

Like any wireless attack, KRACK requires the attacker to be within wireless signal range of the target, and only circumvents the encryption provided by WPA2, not the encryption of the underlying data using Transport Layer Security or other types of protection. (In a proof-of-concept video on his Web site, however, Vanhoef used the SSLStrip tool in combination with KRACK methods to simulate a man-in-the-middle attack to view an Android phone user's encrypted Internet traffic.)

"Attackers can use this novel attack technique to read information that was previously assumed to be safely encrypted. This can be abused to steal sensitive information such as credit card numbers, passwords, chat messages, e-mails, photos and so on," Vanhoef said. "Depending on the network configuration, it is also possible to inject and manipulate data. For example, an attacker might be able to inject ransomware or other malware into Web sites."

Vanhoef began notifying affected vendors in mid-July and had originally planned to go public with details in August, but began working with industry organizations as the scope and scale of the problem became evident.

The coordinated public release of the details of the attack caused a flurry of activity in the security community. A CERT Vulnerability Note #228519 titled, "[WPA2] handshake traffic can be manipulated to induce nonce and session key reuse," went out with a list of 15 affected vendors, including Cisco Systems Inc., Intel Corp., Juniper Networks Inc., Red Hat Inc., Toshiba America Information Systems Inc. and others. Vanhoef's own tests found Android, Linux, Apple OSes, Windows, OpenBSD, MediaTek, Linksys and others vulnerable, although the problems are particularly acute for Android and Linux.

Because of the early notice, Microsoft had already issued fixes for the flaw, a Microsoft spokesperson said in an e-mail: "Microsoft released security updates on October 10th and customers who have Windows Update enabled and applied the security updates, are protected automatically. We updated to protect customers as soon as possible, but as a responsible industry partner, we withheld disclosure until other vendors could develop and release updates."

In a post on his personal blog, Alex Hudson, CTO at Iron Group, ranked his impressions of risk by platform. "Attacks against Android Phones are very easy!" he wrote. "Best to turn off wifi on these devices until fixes are applied. Windows and Mac OS users are much safer. Updates for other OSes will come quite quickly, the big problem is embedded devices for whom updates are slow/never coming."

Hudson also pointed out that the main attack was against clients, not access points. "Updating your router may or may not be necessary: updating your client devices absolutely is! Keep your laptops patched, and particularly get your Android phone updated."

Meanwhile, vendors that are focused on other layers of security were quick to pounce on the incident as further evidence of the need for multifaceted security approaches.

"There's no stopping users from connecting to public Wi-Fi hotspots, so it's up to the enterprise to layer on protection mechanisms. This vulnerability speaks to the importance of ensuring that all connections from endpoints leverage strong encryption, such as the latest versions of Transport Layer Security (TLS). Intermediary proxies can ensure that regardless of what the application supports, all connections from end-user devices leverage strong encryption," Rich Campagna, CEO of Bitglass Inc., said.

FONGLEON356/SHUTTERSTOCK.COM

While WPA2 hasn't been impervious to attack, KRACK represents a significant chink in the armor of one of the more robust quarters of computer security.

While WPA2 hasn't been impervious to attack, the flaw represents a significant chink in the armor of one of the more robust quarters of computer security. Previous attacks on WPA2 mostly involved hitting surrounding technologies, such as vulnerabilities in Wi-Fi Protected Setup (WPS), or required either password guessing or an attack from a table of hashed passwords that could only succeed if the correct password was already included.

It will be possible to issue patches in a backward-compatible manner, meaning that KRACK doesn't create a need for a WPA3, Vanhoef noted. Nonetheless, the combination of unpatched and unpatchable systems mean attacks based on this new method are likely to be a factor in wireless network attacking and defending for a long time to come.

'KNOCKKNOCK' ON THE OFFICE 365 SYSTEM ACCOUNT DOOR

Also this fall, the discovery of a botnet aimed at Office 365 customers put a spotlight on a commonly overlooked category of system accounts.

Skyhigh Networks publicized the finding in October, several weeks after identifying the botnet that it dubbed "KnockKnock." Active since at least May, and especially active from June through August, the relatively small botnet seems to have been highly targeted in both the types of accounts it attacked and the types of organizations it went after.

"The reason this is interesting is not that a botnet is trying to get into accounts, but the fact that it is trying to get into system accounts," said Sekhar Sarukkai, chief scientist at Skyhigh Networks, in an interview.

What the attack does, according to Skyhigh's description, is go after the system accounts that are commonly used to connect the Exchange Online e-mail system with marketing and sales automation software. In cases where the system accounts were compromised, KnockKnock exported data from the inbox, created a new inbox rule and began a phishing attack from the account against the rest of the organization.

Skyhigh picked up evidence of the botnet through its Cloud Access Security Broker (CASB) Threat Protection engine when the company's customers were attacked. Skyhigh says the traffic came from 63 networks and 83 IP addresses, with 90 percent of traffic coming from IP addresses in China. In all, the attacks came from 16 countries.

> "The reason [KnockKnock] is interesting is not that a botnet is trying to get into [Office 365] accounts, but the fact that it is trying to get into system accounts."
>
> *Sekhar Sarukkai, Chief Scientist, Skyhigh Networks*

The attacks averaged only five e-mail addresses per customer. Additionally, the organizational targeting was extremely specific—aimed at infrastructure and Internet of Things (IoT) departments within the manufacturing, financial services, health care and consumer products industries, as well as U.S. public sector agencies.

"It just seems like it's orchestrated in a controlled manner, rather than a free-for-all, get-what-you-can kind of campaign," he said.

Sarukkai said that what's helping the effectiveness of the attack is that non-human system accounts are less likely to be protected by multi-factor authentication or security policies, such as recurring password reset requirements. "Once these accounts have been provisioned, they're really sort of forgotten," he said. "I think these actors have a pretty good understanding of the weakest link in Office 365 and, in general, the security infrastructure—almost like the hidden weakness."

This targeting of system accounts in Office 365 will bear watching for MSPs, whose customers are moving rapidly to the cloud productivity suite.

A TOXIC STEW BEHIND WANNACRY

A toxic stew composed of hacking groups, radical transparency advocates, nation state spies/saboteurs and opportunistic ransomware writers has simmered for the last few years. It boiled over this spring into a messy, costly disaster.

The specifics of the case involve a hacking group called the Shadow Brokers releasing a set of alleged U.S. National Security Agency hacking tools in April. One of the tools was a Windows Server Message Block protocol exploit known as EternalBlue.

Bad actors (suspicion fell on North Korea, but, as is so often the case, no definitive proof emerged) converted EternalBlue into a nasty piece of ransomware called WannaCry. And WannaCry wreaked some havoc when it was unleashed in May, infecting an estimated 230,000 computers and causing problems at hospitals in the United Kingdom. An intrepid security researcher found a kill switch, but variants emerged, and a month later another wave of EternalBlue-based ransomware called Petya struck multiple countries. Again, nation state involvement was suspected, this time with an apparent aim of damaging Ukraine.

Ransomware is a familiar threat, and with Microsoft having released a patch for the flaw underlying EternalBlue in March, the event served as a reminder for the tired, but still necessary, old advice of applying patches ASAP.

But the combination of actors involved here is new. MSPs are used to defending their customers against script kiddies, criminal scammers and corporate spies. Previously, nation-state attackers were only a concern for highly strategic organizations or for the very paranoid. Now MSPs must try to provide advance protection and conduct after-action cleanup on behalf of their customers against nation states and politically motivated groups.

Stuxnet introduced the concept of collateral damage to businesses from a nation-state attack that spiraled out of control, an apparent accident that doesn't seem to have been repeated. The WannaCry episode kicks up the complexity of international cyberconflict. It's a case of apparent non-state instigators with a political agenda mixing it up with an unknown number of groups affiliated with nation states in a shadowy, difficult-to-attribute battle royale with both intentional and collateral damage to computer systems worldwide.

The near-term IT security future promises to be messier and more confusing than it looked just a year ago. Situation normal. •

Scott Bekker is editor in chief of Redmond Channel Partner *magazine.*

GET THE MSP COMPETITIVE ADVANTAGE

Maximize Efficiency with a Best-In-Class RMM and Security Platform

SolarWinds MSP empowers MSPs of every size and scale worldwide to create highly efficient and profitable businesses that drive a measurable competitive advantage. Integrated solutions including automation, security, and network and service management—both on-premises and in the cloud, backed by actionable data insights, help MSPs get the job done easier and faster.

SolarWinds MSP helps MSPs focus on what matters most—meeting their SLAs and creating a profitable business.

FOR MORE INFORMATION,
visit solarwindsmsp.com

Or call +1 (919) 957-5099

SolarWinds® RMM

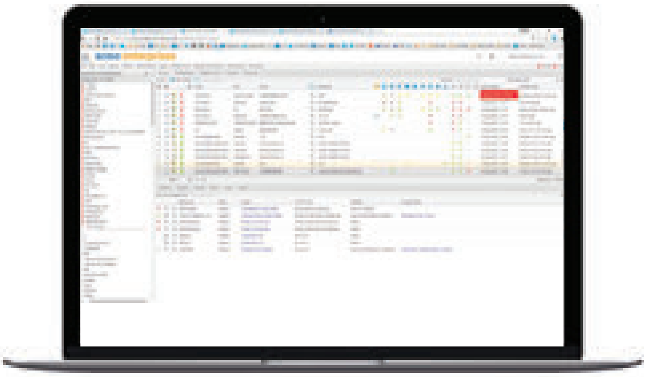
SolarWinds® Backup

SolarWinds® MSP Manager™

SolarWinds® Mail Assure™

SolarWinds® Risk Intelligence

SolarWinds® MSP Anywhere™



solarwinds
msp