SIM2K
Adapting Technology to Your Business Needs

6•17
Information you can use

SIMformation

New Approach to Malware Prevention

For many companies, protecting their network from malware attacks is in flux. Anti-virus (AV) programs work for those already-identified threats where the company has had time to work up a defense against that threat. But what about zero-day attacks, those released before an AV company can release a defense? And, what about malware like ransomware that comes in through e-mail hidden in a document? Obviously there needs to be yet another line of defense.

Most enterprises deploy a traditional "detect and respond" anti-virus solution that leaves their systems open to continual attacks. They face a constant, reactive cycle that drains resources, leaves them open to regulation violations and can impact brand reputation and their bottom line. What most enterprises that suffer a serious breach wish they had known is that their security infrastructure should have been made up of not just traditional antivirus solutions, but a product that relies on artificial intelligence and algorithmic science to detect and quarantine threats BEFORE they cause harm and a set of customized deployment and remediation services that optimize the operation of their entire security strategy.

SIM2K has taken on that challenge and is now offering what many believe to be the next step against malware – Future-Proof Endpoint Security. We are now offering our clients CylancePROTECT®.

CylancePROTECT prevents malware before it can execute, including system- and memory-based attacks, scripting, spear phishing, zero-day malware, privilege escalations, and malicious and potentially unwanted programs.

CylancePROTECT redefines what anti-virus can and should do for your organization by leveraging artificial intelligence to detect AND prevent malware from executing on your endpoints in real time. By taking a mathematical approach to malware identification utilizing patent-pending, machine learning techniques instead of reactive signatures and sandboxes, CylancePROTECT renders new malware, viruses, bots, and unknown future variants useless.

Cylance® has developed the most accurate, efficient and effective solution for preventing advanced persistent threats and malware from executing on your organization's endpoints. At the core of Cylance's malware identification capability is a machine learning research platform that harnesses the power of algorithmic science and artificial intelligence. It analyzes and classifies hundreds of thousands of characteristics per file, breaking them down to discern whether an object is good or bad in real time.

CylancePROTECT's architecture consists of a small agent that integrates with existing software management systems or Cylance's own cloud console. The endpoint will detect and prevent malware through the use of tested mathematical models on the host, independent of a cloud or signatures. It is capable of detecting and quarantining malware in both open and isolated networks without the need for continual signature updates.

Defense requires applying the best protection at the most vulnerable locations - the endpoints. Cylance's mathematical approach stops the execution of harmful code regardless of having prior knowledge or employing an unknown obfuscation technique. No other anti-malware product compares to the accuracy, ease of management, and effectiveness of CylancePROTECT.

The protection comes from a lightweight agent uses only 1-3% of PC processing power - 10 times fewer system resources than traditional endpoint security solutions - to provide superior, preventive protection. CylancePROTECT is compatible with all current versions of Microsoft Windows and macOS, and can also be added to other devices such as smartphone and other appliances such as those categorized as part of the Internet of Things (IoT). This way, your protection extends out to any device that might connect to your network in any way.

SIM2K takes security very seriously, and we are always looking for innovative products such as Cylance that can give our clients additional protection. We will be rolling out Cylance to our Pinnacle customers, and we will make it available to all interested clients on a per-device basis, so contact us for more information.

We would also note that SIM2K offers many security services such as network evaluations, employee training and best-practice reviews. For example, we offer "spear-phishing" tests, wherein we spoof a malware attack by sending your employees an e-mail. If they click on the links in the e-mail, we will know and that employee can be counseled on how best to look out for phishing e-mails. But, your network has not been compromised like with a real attack. We offer consulting to help you develop a security program that covers both technology and people and is right-sized to meet the specific needs of your company. Please contact us to schedule your demonstration of CylancePROTECT today!

CYLANCE

On-Line Password Firm Breached

Encrypted information has been accessed during a data breach at password management service OneLogin. It affects "all customers served by our US data center" and perpetrators had "the ability to decrypt encrypted data", according to news sources. Those affected have been advised to visit a registration-only support page, outlining the steps they need to take.

Security experts said the breach was "embarrassing" and showed every company was open to attack. OneLogin is a single sign-on service, allowing users to access multiple apps and sites with just one password.

Apps and sites integrated into the service include Amazon Web Services, Microsoft Office 365, Slack, Cisco Webex, Google Analytics and LinkedIn.

"We have since blocked this unauthorized access, reported the matter to law enforcement, and are working with an independent security firm to determine how the unauthorized access happened," said OneLogin's chief information security officer. "We are actively working to determine how best to prevent such an incident from occurring in the future."

Users who log in to the site have been given a list of steps designed to minimize the risk to their data. These include:

- forcing a password reset for all users
- generating new security credentials and certificates for apps and sites
- recycling secrets stored in OneLogin's secure notes

Some customers have criticised OneLogin for requiring users to log in to see the list.

In its e-mail to customers, OneLogin told them that "because this is still an active investigation involving law enforcement, there are certain details we can't comment on at this time. We understand how frustrating this might be and thank you for your patience while we continue the investigation."

"Companies need to understand the risks of using cloud-based systems," said a security expert. "Increasingly they need to encrypt sensitive information before they put it within cloud systems, and watch that their encryption keys are not distributed to malicious agents. It is almost impossible to decrypt data that uses strong encryption, unless the encryption key has been generated from a simple password," the security officer said.

Another IT security consultant said it was likely the compromised data included passwords protected using "hashing" - converting the data into fixed-length strings of characters or numbers. "The security of data would then depend on the strength of the passwords, and of the password hashes. I would happily store my properly encrypted password safe in any cloud service, because you don't know my password for that safe and I trust encryption."

This breach points out the potential dangers of using a password management site in the Cloud as it does put all your login information into one handy basket for the "bad guys" to access. Call SIM2K for information on password management tools.

Windows 7 Hangs Tough

Windows 7 last month dug in its heels, and retained control over a majority of all Windows PCs, an analytics company reported. May's Windows 7 user share – an estimate of the percentage of the world's personal computers powered by the 2009 operating system – was 49.5%, said metrics vendor Net Applications. However, Windows 7 ran 54% of all Windows machines: The difference between the user share of all PCs and only those running Windows stemmed from Windows powering 91.6% of the globe's personal computers, not 100%.

More importantly, Windows 7's share has barely moved in the last 12 months, dropping less than one percentage point in that time. As a portion of Windows personal computers only, Windows 7 has been just as obstinate: Its share has stayed near 54%.

The lack of a decline in Windows 7's user share over such a long stretch may signal trouble ahead as customers try to beat the end-of-support deadline, set for January 14, 2020. Windows 7's current status, in fact, is comparable to that of Windows XP 31 months before its April 2014 retirement.

At the time, Windows XP powered 54.6% of all Windows PCs, nearly the same as Windows 7 did in May. That is significant because as XP's support deadline approached, many businesses busted budgets to purge Windows XP systems from their networks. They bought new PCs, brought in outside help to tackle the migration, disrupted existing IT plans and schedules, and purchased costly custom support plans in last-minute efforts to keep their machines secure.

Even so, massive numbers of Windows XP – left vulnerable because Microsoft halted patch delivery when support expired – continued to run in enterprises. According to surveys by Gartner in 2014, nearly 25% of the PCs in organizations – private enterprises, government agencies and the like – were still running XP when Microsoft pulled the patch plug. Net Applications pegged Windows XP's user share at 29% of all Windows PCs in April 2014.

Contrary to more recent commentary from Gartner, which asserted that enterprises are further into Windows 10 migration than the previous Windows XP to Windows 7 transition, the data from Net Applications does not show any indication of companies moving forward with migrations to Windows 10. Current estimations have Windows 10 accounting for only 29.2% of all Windows PCs in May, up some from the month prior, while Windows 8/8.1 and the long-outdated Windows XP both lost share, falling to 9.1% and 6.2%, respectively.

SIM2K continues to support Windows 7, as well as Windows 10. But, for planning purposes, we just want companies to be aware of the 2020 date when budgeting IT needs in the next few years.

SIMformation is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 75th St., Suite 336, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

Biometrics to Replace Passwords?

Headlines about mass data breaches have become ominously routine, and yet password convenience still trumps security for most people. That's why, year after year, the world's most popular log-on remains "123456," a password so obvious it accounted for 17% of the 10 million compromised passwords analyzed by Keeper Security, which sells a log-in management service.

One answer is to get rid of passwords altogether. Biometric technology – especially fingerprint scanners – has been steadily replacing the need to type in a password, which can easily be guessed by hackers wielding smart algorithms. Now, with more voice-activated devices like the Amazon Echo, companies are starting to create technology that recognizes a person's speech patterns. Facial recognition is beginning to catch on as well.

The question is whether companies will be able to persuade people to switch to biometric log-ins and whether the new technology will prove any more resistant to hackers than the old-fashioned password.

In March 2015, Yahoo began a process to cut out the need for customers to remember a password to log into its e-mail service. Users could be sent a one-use-only random password via SMS to their cell phone instead. In October that year, the company expanded this functionality to take advantage of smartphones. Instead of typing a password, a user's phone can be sent a notification asking them to just confirm the login attempt was legitimate. As many smartphones now feature biometric sensors, this method can be more secure still than an SMS, as it not only requires a phone to be present, but it must also be unlocked by the user.

Systems such as this have been made possible in large part by Apple, which popularized the fingerprint scanner by embedding it in the iPhone four years ago, and subsequently added it to the MacBook lineup. Microsoft is also getting into the act. The banking industry, long mindful of security, has adopted some of the most cutting-edge technology. The U.K. bank Barclays started letting wealthy customers verify their identity during telephone banking with their voices back in 2014, and rolled out an opt-in version to retail clients last year.

Face recognition is becoming more common as well. Lloyds Banking Group it trialing Window's Hello technology, which lets online users log in by pointing their face into a computer's webcam.

Is the new technology hacker-proof? IT experts are up in the air in this regard. Some point out to speech synthesis tools like Lyrebird which can mimic anyone's voice. Some facial recognition systems have been fooled by holding up a picture of the user for the webcam scan.

However, it is obvious that the IT industry is taking the issue of security seriously in seeking a replacement for passwords. But old habits die hard, and breaking this reliance will take time. After all, do you still have a landline phone at home? But new techniques should provide added security, helping to keep the bad guys at bay a little longer with each new development.

"Random Tid-Bytes"

Intel Compute Stick

Chip maker Intel has released a handy new "computer on a stick" that offers some interesting possibilities. This is a fully-configured computer that looks like a USB flash drive. But, it has either an Intel Atom or CoreM processor with up to 4 GB of memory and 64 GB of on-board storage. It even has a mini-fan for cooling. It plugs into a HDMI port on a TV or monitor and is a fully functional computer. Intel is positioning this as a way to create thin-client computers for kiosks or classrooms, or a way to provide content for home entertainment systems or digital signage. It supports wireless connectivity and runs either Windows 10, 8.1 or Linux. Pricing starts at around $130 and up depending on processor, memory and operating system. One interesting use would be for those "road warriors" who travel but don't want to have to carry a laptop along. This little gizmo can take the place of that bulky case/PC/power brick into a device the size of a pack of gum!

Need a Printer?

In this day of desktop publishing, companies often forget that some times they need something actually – printed. We are talking about the printing press type of printer here, not a HP ink jet device. Many of our clients have specialized forms (yes, the multi-part carbonless paper form still exists) or want the look and feel of embossed logos on letterhead. Or, they need roll labels, continuous-feed forms or marketing materials printed with die-cuts and varnishes. What you may not know is that SIM2K has relationships with printers to get these types of print jobs done. We can help you specify your print project (paper weight, inks, bindery, finishing, etc.), obtain printing quotes, help prepare files for the printer and manage the project on-press. To date, we have found our printing sources to be very competitive for pricing, so if you have a need for "traditional" printing, and don't know where to start, give SIM2K a call!

The Selfie Economy?

You may not have recognized it, but the most obvious business impact of selfies is marketing. Instead of advertising, companies are increasingly staging "instagrammable experiences" and letting customers spread the good word. When you add up the selfie-driven identity economy, the selfie-driven experience economy and selfie-driven marketing, you get something like a selfie industrial complex – a new world of business opportunity that is emerging out of the selfie impulse that has arisen in the past 10 years. Whether this opportunity will be worth a trillion dollars or a hundred trillion dollars, nobody knows. Selfies posted on social media express "self" even better than products do. But to get the best selfies, you have to spend on restaurants, vacations and other experiences that enable pictures to show the consumer in the best possible light capturing special moments in beautiful places. Understanding this shift of self expression from brand association to social photography is a major key to how innovative marketing is succeeding.

Fallout from WannaCry Ransomware Attack Continues

Last month Microsoft took the unprecedented step of issuing security patches for Windows XP, an operating system taken out of support more than three years ago.
The decision to help PCs running XP, as well as Windows Server 2003, was intended to slow the spread of the WannaCry ransomware, which encrypted files on hundreds of thousands of PCs world-wide.

WannaCry's rapid spread was credited to its exploit of a Windows vulnerability, one that Microsoft had patched in March on still-supported versions, such as Windows 7 and Windows Server 2008. But after WannaCry wreaked its havoc and Microsoft reversed its long-standing policy against free fixes for older operating systems, the IT industry had questions, both about the criticism aimed at seemingly every party except the attackers, as well as what Microsoft's release of patches portended.

Computerworld, an on-line IT magazine, put those questions to two patch experts, and their answers were interesting:

(Q) What does Microsoft owe users of retired products when a serious event occurs, as with WannaCry? Does it owe them patches in most cases? Every case? Some have argued that it does.
Expert 1: I don't think Microsoft owes us patches. We have a clear support statement. We can purchase support if we choose to. We clearly have decided that the risk of being unsupported was acceptable. We made the decision. Now we are paying the price (literally, in some cases).
Expert 2: In the case of retired software, Microsoft doesn't owe their customers anything. One of the challenges of being a vendor is that you do need to move your products forward, and maintaining old platforms becomes a resource drag, acting like a sea anchor. Anyone who wants to stay on an older platform can, and Microsoft has created extended support programs for customers who wish to keep those platforms secure.

(Q) Post-WannaCry, critics blamed, among others, IT administrators for allowing out-of-support systems to remain in use. What circumstances and conditions impede retiring older operating systems or products? Why do firms keep running, say, Windows XP, when everyone knows that they are insecure?
Expert 1: A combination of lack of resources for upgrades, or there is no comparable product to upgrade to that gives you equivalent functionality. It takes time and resources to test and ensure that there is vendor support, ensuring that your current software works with it. [Or] the device may [run] Windows XP Embedded, and thus you have to buy a whole new device, not just upgrade the hardware.
Expert 2: No one group holds the blame. In many cases the business holds IT back by holding on to legacy systems that cannot run on newer platforms. In some cases, the cost to update the backend system may be significant, forcing the endpoint to remain on a system that is now out of date or – if it is highly customized or built by a company that no longer exists – it may be down to staying on the old system or having to migrate a business-critical system to an entirely new platform.

(Q) Other critics panned companies that had not deployed the March security updates to still-in-support Windows PCs by the time WannaCry hit. But what is an "average" patch time among Microsoft's commercial customers? Is it legitimate to expect a business to be fully patched 60 days after updates are available? 30 days? 90 days?
Expert 1: Normally, for good patchers, I see a lag of no more than 30 to 60 days. But this pointed out we still suck at getting updates installed – even in places where the servers should be managed and maintained.
Expert 2: I have seen stats over the years ranging from 60 to even 120 days. What we recommend is to ensure critical OS updates get rolled out within two to four weeks. Applications that are highly targeted (Chrome, IE, Firefox, Flash, Adobe Reader, Office) in two weeks or less. We know it can be done and see companies doing it ... in complex environments across tens of thousands, and in some cases hundreds of thousands, of endpoints.

(Q)Will offering patches for products out of support get more complicated once Windows 10 has gone through several additional upgrades? What will Microsoft do if, say, a serious security event occurs early next year that impacts versions that have been knocked off the support list? By January 2020, when Microsoft retires Windows 7, six versions of Windows 10 will have fallen from support. What happens if a critical threat occurs then?
Expert 1: The people I've seen struggling the most with getting patches installed aren't even on Windows 10. So, the first thing that Microsoft needs to do is still address what is keeping us off of Windows 10. Once we're there, then they need to ensure better compatibility and lack of issues between the releases. But to answer the question, as many times as Microsoft annoys me with their seemingly heavy-handed actions, remember that people in a conference room make the decision. And every time one of these events happens where customers are really getting hurt, Microsoft does the right thing and protects us.
Expert 2: I think Microsoft plans to be more aggressive with End-of-life of older versions of Windows 10. I am not sure we can expect them to do the extended support as they have done in the past. They established the Long-term Servicing Branch for that purpose. You either need to adopt that from the beginning or get on the treadmill and keep up with the upgrades.

The furor over WannaCry seems to have abated as the IT industry rushed to patch computers and head off further infections. However, this incident and the discussion above shows the importance of a good Patch Management program for your company's hardware. SIM2K offers a comprehensive program for managing your patches, so if you are not a current SIM2K Pinnacle or Serenity customer, contact us for more information on how we can assist you with this vital function.

Computerworld, June 12, 2017

SIM2K
6330 E 75th St., Suite 336
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com