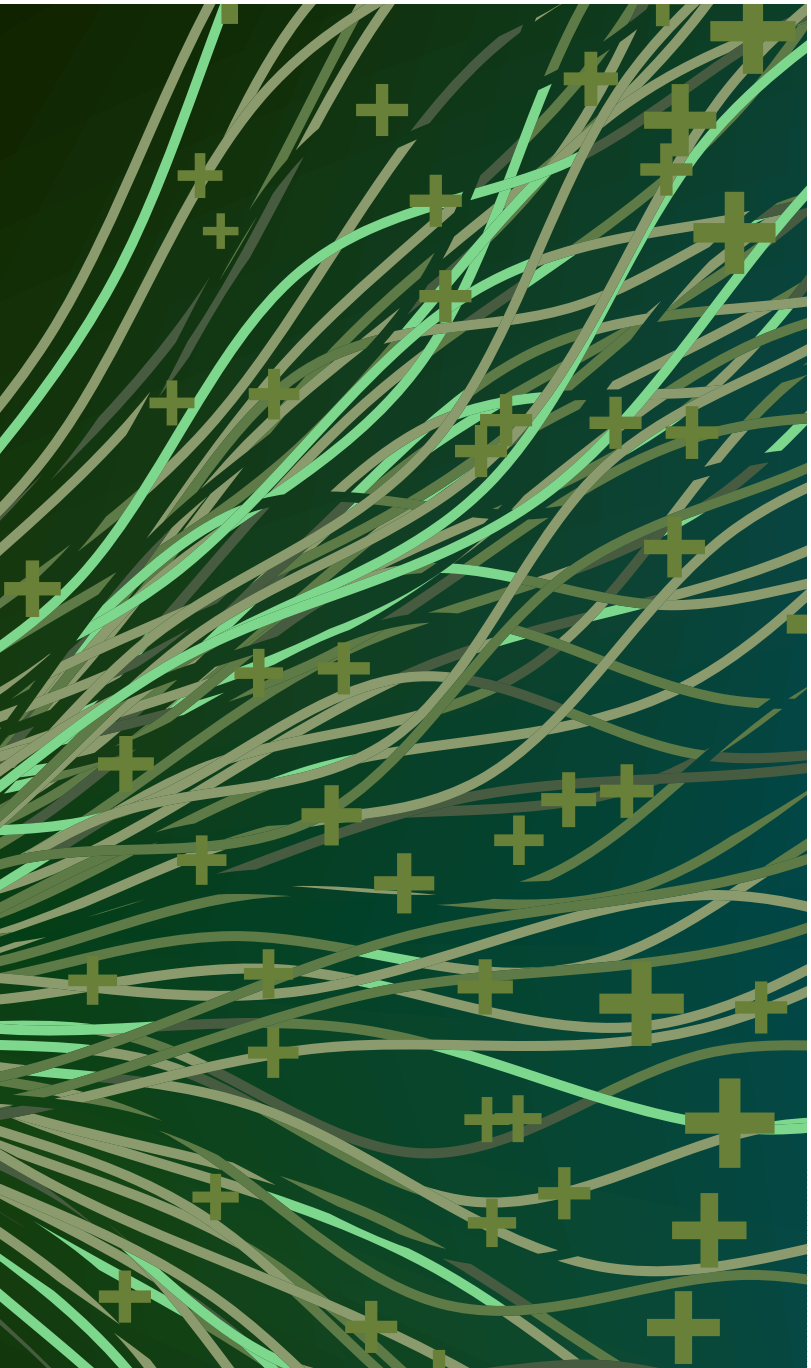

E-Guide

DEFENDING AGAINST THE DIGITAL INVASION

TechTarget | SearchSecurity

THE CONFLUENCE OF the Internet of Things and BYOD may turn into a beachhead for attackers. Johannes Ullrich, SANS Institute CTO and head of the Internet Storm Center, outlines the top emerging cyberthreats in 2015, from the Internet of Things and bring your own device to subtle data manipulations that influence business decisions and enterprise ransomware.

DEFENDING AGAINST THE DIGITAL INVASION

Johannes B. Ullrich

It's hard to forget the publicized data breaches of the last few years that upended the fortunes of victimized organizations. Target Corp. attributed $148 million of losses to the breach it suffered. Anthem Insurances Companies Inc. failed to protect millions of healthcare insurance subscribers' Social Security numbers. Sony Pictures Entertainment Inc. has had its internal communications exposed and data wiped off its hard drives. Despite the fallout, in 2015 many security officers will continue to focus on improving the security operations and risk management processes they have in place, with a watchful eye toward business risk and emerging cyberthreats.

Networks are only going to become more complex, increasing the attack surface and moving large parts of the infrastructure outside of corporate control. The confluence of the Internet of Things and bring your own device (BYOD) will start to invade enterprise networks in new ways. Attackers will learn to take advantage of these exposures.

Home

Defending against
the Digital Invasion

Today little data is lost in most Web defacements. And the attacks, in general, are clearly visible. Security teams can expect to see more dangerous attacks that are harder to detect in the coming months. Some miscreants may not rely on data exfiltration at all, but instead apply subtle manipulations to data processing systems to influence business decisions.

Up to now, actors using distributed denial-of-service (DDoS) attacks had little reason to innovate. With an ample supply of compromised systems and reflectors available in large numbers to obscure and amplify the attacks, they were able to flood networks with simple requests. However, defensive techniques have improved and anti-DDoS services have become quite capable of stopping all but the largest attacks. DDoS attacks blending in with normal requests that require significant resources to process are much more difficult to block. While cloud-hosted applications may absorb the additional loads, dynamic pricing models could cause significant financial burdens for organizations that come under attack.

We saw criminals perfecting crypto ransomware in 2014. These activities—in which attackers infect systems, encrypt the data and hold it "hostage" until their demands are met—typically targeted consumers and small businesses; this threat has only affected enterprise networks peripherally. But the attackers

had significant financial success with these "data kidnapping" methods. The next-generation of crypto ransomware will become more furtive—maintaining business continuity for months after the initial infection takes place. This will ensure that not only current data but also many recent backups are encrypted once the attacker decides to remove the key to ask for the ransom.

When responding to these attack techniques, security teams will have to account for more complex networks. Understanding your infrastructure, defenses and how they are affected by these attack methods, is critical in order to provide guidance about your organization's current risk profile.

INVASION OF DIGITAL THINGS

Most CISOs have already faced some challenges as traditional workspaces continue to morph into work from anywhere on a myriad of devices. For years now, office space has shrunk as more work is being done from employees' homes. But just as work is no longer separated from our personal lives, consumer technology such as wearables and home monitoring systems are invading the enterprise. BYOD was just the beginning.

Consumer-grade devices, which are not included in centralized IT management initiatives, will more and more become part of corporate networks.

Charging stations for electric cars, fitness monitors included in corporate health plans, devices to monitor and control home security systems, and smart watches will all be connected to corporate networks, like smartphones and tablets before them. But the difference is that these devices will provide even fewer safeguards and far less visibility into their internal workings. None of these devices will connect to enterprise authentication systems, and the network stack and the number of supported operating systems will be more diverse.

A simple move to replace an old-style television in a break room with a smart TV will expose your network to new threats. This "IT device" will now be connected to your network. At the same time, it will be receiving wireless signals over the air in the form of digital TV transmissions, infrared remote control signals and, maybe, even offering Wi-Fi and Bluetooth connectivity while providing new gateways into your infrastructure. It will not integrate with existing patch management and access control systems.

At this point, we are just starting to understand the threats that we are being exposed to—due to the buggy and incomplete security controls these devices are prone to provide. These devices can easily turn into a beachhead that an attacker can use to completely compromise your network. Proper onboarding, network segmentation and testing of these devices will be critical,

but these processes have to be developed to scale. Policy alone will not protect you in a world where a smartphone contains four or more different radios, and a watch supports at least two.

Just like Target's network was breached via its heating and ventilation system, the next large credit card breach may originate from a smart watch or a smart TV. In 2014, a number of network-connected security cameras were breached (see figure) giving attackers access to corporate networks. Later these cameras were used to scan for network-connected storage devices.

Similar to USB thumb drives of the past, these devices will connect and exchange data with corporate technologies, and potentially introduce malware into our networks, bypassing legacy chokepoint-focused perimeter controls. To detect these threats, controls must be able to monitor lateral movement, and they need to be applied continuously to identify threats quickly. Even if these devices do not have the ability to send and execute files remotely, they may still have access to corporate APIs that can be used to manipulate data and influence business decisions.

SUBTLE MANIPULATION, HIGH COST

Because untrusted devices can gain access to internal APIs, you are now faced with increasingly subtle and difficult-to-detect attacks. You may still see defaced websites and large leaks of customer data and intellectual property. But in hindsight, you may wish these large, visible threats were all you had to worry about. A defacement of a public-facing website may temporarily damage your company's image, yet it is easily detected and relatively straightforward to resolve. Leaking customer data may require dealing with regulators, and your company may endure significant costs in remediating the breach. Still, despite the headlines, most companies still recover, and even thrive, after large data breaches.

That wasn't the case for a CEO whose company was pushed to the brink of bankruptcy after losing a number of high-profile bids to a foreign competitor. Not because its product was worse, but because its price was too high. The price his team quoted was based on a cost estimate derived from an internal enterprise resource planning system. What was the problem? The pricing data was manipulated by malware to provide the wrong results, and the changes were so subtle they were not easily detectable. The outcome was an overstatement of the cost for these projects. No modern business or government today can

Home

Defending against
the Digital Invasion

make decisions without using data analytics, and accurate results are critical. These breaches also escape the public eye because they do not result in the loss of customer information, and the culprits are long gone by the time these breaches are discovered, if they are even detected at all.

DDOS MOBILIZES

Denial-of-service attacks, on the other hand, are easy to spot, but can be difficult and expensive to fight. Over the last few years, we saw the size of DDoS attacks climb significantly. Attackers perfected the ability to collect large numbers of compromised systems and turn them into powerful weapons by amplifying their output using protocols like DNS, SNMP and NTP. While these attacks are powerful and can lead to enormous traffic floods, they can be identified and filtered using specialized anti-DDoS services. Even small to medium-sized businesses are now used to paying thousands of dollars per month for "DDoS insurance."

As a result of better defenses, attacks these days often go unnoticed. And, in particular, large financial companies that were targeted heavily in the past have learned to live with DDoS attacks and experience little disruption as a result. Future DDoS attackers may take a step back and not just flood the network

Home

Defending against
the Digital Invasion

infrastructure. Instead, by targeting specific application-layer resource bottlenecks, attackers may try to send fewer but smarter requests that fit in with normal queries and are harder to filter.

Mobile APIs often do not include sufficient rate limits and are easily exploited to launch DDoS attacks. If the attacks use compromised mobile devices as a launch platform, they are very difficult to distinguish from valid requests and can easily overwhelm a back-end database. In some cases, it may not even take a full compromise of the device.

Many APIs encourage third-party developers to take advantage of the programming interfaces and, with that, allow and support cross-origin requests from other Web applications. In this case, all it takes is some JavaScript on a popular website to build powerful ad-hoc attack networks that will send requests, which are indistinguishable from valid inquiries.

RANSOMWARE AT WORK

Over the last few years, we have seen crypto ransom-ware affect consumer, as well as enterprise, desktops. CryptoLocker and similar malware have locked thousands of systems and generated millions in revenue for the miscreants behind it. In the future, we should expect to see more ransomware affecting

servers. That includes sophisticated and stealthy varieties that will infect a network for months before divulging that valuable data was encrypted and is no longer accessible unless a large amount of money is paid.

This type of ransomware usually implements a shim between the application and the data store. The data is encrypted and decrypted on the fly, without the application noticing. In some ways, this malware mimics security software that implements database or full disk encryption without disrupting the normal operation of the system. Once the attacker believes enough data is encrypted, the key is removed and the application will fail, asking for a ransom payment to retrieve the key. If the encryption happened for long enough, backups are presumed to be encrypted and unusable as well. The key is often only stored remotely or in memory on the affected system, making it unlikely to be recovered; and even if the malware is detected, it is very possible that the key will not be recovered. With the large financial success gained from desktop crypto ransomware, server-based versions will become more common and even more devastating.

From a defensive point of view, all these threats require a thorough understanding of the network that needs to be protected, consistent controls to enforce security policy and continuous monitoring for compromise. Detecting

compromise quickly, understanding the complex interactions between systems correctly to properly contain the compromise and following well-rehearsed incident playbooks is essential. In many ways, it is more important to do what you do now right, instead of looking at new technologies that may further complicate your network defenses.

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.