



The Four Current Threats Enterprises Can't Ignore

By Jaikumar Vijayan

**SECURITY
BOULEVARD**

Enterprises constantly have to refine and update their security controls to stay ahead of cyberattackers. Digital transformation and the adoption of cloud and mobile computing technologies have given attackers new ways to steal data, to disrupt and to destroy. Just as quickly as defenders have been able to put in place controls against new and emergent threats, attackers have found ways around them.

To be effective at security these days, organizations need to think beyond perimeter protections. Few enterprises realistically can expect to stop 100 percent of the attacks directed at them, because adversaries simply have too many avenues and opportunities to carry out malicious activities.

The cloud has scattered enterprise data way outside the network perimeter and mobile technologies have given employees, partners, suppliers and others the ability to access it from any place at any time. In the next few years, the attack surface will only become broader as organizations begin deploying more internet-connected devices to track assets, manage fleets, monitor data centers and myriad other reasons.

Many of the biggest cybersecurity threats that organizations face currently take advantage of, or are the direct result of, these trends. They exploit weaknesses in technologies, processes and deployment and are testing the ability of enterprises to detect, protect against, respond to and mitigate attacks.





UPDATE

Ransomware Rising

Ransomware attacks, in which adversaries encrypt crucial data and demand money for the decryption key, have emerged as a major threat to enterprises over the past year. Organizations that don't have robust data backup and recovery processes are at particular risk. The only option for most of them is to either pay — and risk inviting more attacks — or lose data.

Last year, 26 percent of all ransomware attacks were directed at businesses. That was up marginally from 23 percent a year ago, according to [Kaspersky Lab](#). Another security vendor, [Barkly](#), has estimated that at least 15 percent of organizations across 10 separate industry sectors including health care, financial services and education have been attacked in ransomware campaigns. Many of the victims were organizations with more than 1,000 employees.

According to [Barkly](#), a business is hit with ransomware every 40 seconds, and the average ransom demand is now more than \$1,000. Some have paid tens of thousands of dollars to get their data back.

Gartner analyst Avivah Litan says ransomware attacks will grow at double-digit rates this year, fueled by the growing availability of low-cost attack kits and hosted services in underground forums. Increasingly, ransomware attacks will be targeted at enterprise data in the cloud.

Ransomware attacks focus attention on the need for organizations to regularly back up data. Often, the only way for a victim to avoid paying a ransom is to have recent backup copies of any data that the attackers might have encrypted.

In recent attacks, adversaries have begun encrypting not just data files but also shadow copies and Windows System Restore points that can be used to restore data following a ransomware attack, warns Carnegie Mellon University's [SEI CERT](#). Therefore, backups need to be stored on separate offline systems and updated regularly to ensure data can be restored following an attack. Restricting code execution on end user systems, decreasing user accounts and limiting administrative access on systems also can limit the damage, according to CERT.

From a delivery and distribution standpoint, ransomware is no different from most malware. Most of the time, it is delivered on host systems via email and drive-by downloads. But researchers have observed an increase in the use of other tactics as well, including the use of stolen credentials and brute-force attacks on RDP to deliver ransomware. Some samples, such as WannaCry and NotPetya, are designed specifically to self-propagate on enterprise networks via SMB shares. Organizations that conduct regular employee training, keep their anti-malware tools up-to-date and employ standard mechanisms for email filtering can reduce some of their exposure to the threat.

Beyond such measures, ransomware attacks require enterprises to think about the value of their different data classes and whether or how much they would be willing to pay to get it back if no other option is available. When planning for ransomware attacks, organizations must decide if payment is something they would be willing to entertain. Factors including ransom negotiations and getting quick access to bitcoins to pay off attackers are important as well. Some enterprises already have begun [stockpiling bitcoins](#) as part of their strategy to regain access to their data if they were to be attacked.



Last year, **26 percent** of all ransomware attacks were directed at businesses. That was up marginally from **23 percent** a year ago



A business is hit with ransomware every 40 seconds



The average ransom demand is now more than \$1,000





Imminent IoT Threats

Botnets built from insecure consumer internet of things (IoT) devices such as smart TVs, wireless IP cameras and DVRs pose a big threat to enterprise security, as the Mirai DDoS attacks in late 2016 showed. But consumer devices are not the only enterprise IoT security concern. The many internet-connected sensors and devices that organizations have begun deploying for applications such as asset tracking, factory floor monitoring and process control pose growing risks as well. Gartner expects that by 2020, enterprises will deploy more than 7 billion IoT devices in a wide range of applications including business-to-business ones.

Like consumer products, many of the IoT devices organizations are using in enterprise settings have weak or non-existent access controls and often don't support security patching or over-the-air updates. Security departments often have little visibility over these devices or the extent to which they have been deployed across the enterprise, says Patrick Daly, an analyst with the 451 Group.

To adversaries, these devices can provide an entryway to the broader IT and OT network. Enterprise IoT devices also present a target for exploitation themselves. Organizations including the [IoT Forum](#) have warned about the potential for attackers to lock up weakly protected IoT devices and demand a ransom to unlock it, just as they are doing currently with data files. There's a third risk as well: Attackers can take control of poorly secured enterprise IoT devices and use them to launch attacks against other entities relatively easily.

"Today we have these new unmanaged devices of all types connecting via Wi-Fi, Bluetooth, Zigbee and more," says Yevgeny Dibrov, CEO and co-founder of Armis. Many of them don't support traditional security agents and patching. Additionally, updating the operating systems on these devices can be enormously challenging for a variety of reasons. In essence, what this means is that enterprises are deploying devices that are vulnerable, cannot be easily protected and are accessible over the internet, Dibrov says.

"The best approach for enterprises to mitigate the risk posed by their IoT devices is to apply basic security hygiene rules," 451 Group's Daly says. That means changing usernames and passwords regularly and only purchasing devices that are capable of receiving over-the-air updates. It also means maintaining an updated inventory of network-connected devices and their characteristics to cross-reference with vulnerability databases. Enterprises should be paying attention to closing any network ports that aren't necessary for the device's normal functionality, Daly says.

"The best approach for enterprises to mitigate the risk posed by their IoT devices is to apply basic security hygiene rules."

***– Patrick Daly
451 Group***

The fact that most IoT devices have a limited set of expected normal behavior and communications also makes it easy to spot trouble, he says. "Passive network monitoring tools that leverage behavioral analytics to alert to abnormal activity have emerged as a useful method of quickly identifying and responding to IoT-related threats."

DDoS Disruptions

Distributed denial of service (DDoS) attacks have become bigger, more complex and more frequent than before and remain a major enterprise security concern. Among the major factors driving the trend are the growing availability of DDoS-for-hire services, the proliferation of mobile and IoT botnets and criminals trying to extort money from enterprises by threatening to disrupt their operations.

Threat actors who once relied largely on infected Windows desktop systems to launch DDoS attacks these days have a vast and growing pool of poorly protected IoT and mobile devices to use instead. Botnets assembled from these devices — such as Mirai, Reaper and Satori — have recently begun giving threat actors the ability to launch terabit-scale DDoS attacks. A new emerging class of mobile botnets — including 2017's WireX Android botnet — is adding to the firepower that threat actors have at their disposal these days to launch DDoS attacks.

Size and scale are not the only concerns. Attackers also have begun shifting their tactics to bypass DDoS mitigation countermeasures. With many enterprises scaling up their mitigation approaches to handle bigger DDoS volumes, attackers have begun employing new methods to break through, says Igal Zeifman, security evangelist for Imperva.

"In the past year, we saw two dominant new trends," Zeifman says. "The first was an increase in the number of DDoS attacks consisting of multiple short and powerful bursts, which strike targets persistently and in rapid succession. The goal, he says, is to overwhelm mitigation controls. The net result was that DDoS attacks became shorter and more persistent in the third quarter of 2017 with more than 69 percent of network layer attacks lasting less than 30 minutes.

"The second trend we saw was an increase in the use of high packet-rate assaults, in which the target — or the mitigation solution that protects it — has to deal with a massive amount of DDoS payloads each second," Zeifman says. Some of the attacks scaled as high as 650 million packets per second and were designed to overwhelm the processing capacities of any mitigation service that an enterprise might be using.

"The common thread between the two trends is that they both relate to new attack MOs, meant to circumvent DDoS mitigation solutions," he notes.

For the same purpose, attackers also have begun combining network and application layer attacks. Many DDoS attacks last year were multicomponent attacks that combined HTTP flood, UDP flood, SYN and TCP connect attacks, according to Kaspersky Lab.

The trends highlight the need for organizations to pay more attention to their DDoS mitigation vendor's capabilities, says Joseph Blankenship, an analyst at Forrester. "You want to know how many scrubbing centers the vendor has for stopping DDoS attacks," he says. Organizations should make sure the vendor has locations in geographies where they have operations. They also need to pay attention to the vendor's DDoS traffic-scrubbing capacity. "Look for vendors that have scrubbing capacity in excess of the largest attacks we're seeing. Many vendors are designing their networks to defend against attacks 3-5 times larger than the largest attack," he notes.

Also important to find out are how many security operations centers the DDoS mitigation center has and the number and quality of their staff. "You want to know that in times of crisis, you have experienced professionals ready to support you," Blankenship says. "Some services can be deployed in minutes to stop attacks in progress."

More than 69 percent
of network layer attacks
last less than 30 minutes



Attacks can scale as
high as 650 million
packets per second





Mobile Malevolence

Smartphones and tablets have become a bigger target for attackers simply because of how ubiquitous their use has become in recent years.

For enterprises, mobile devices pose a two-pronged threat: Their increased use to access enterprise applications and data has heightened data loss risks, and vulnerable mobile devices can provide an entry for attackers to the broader IT network.

Every organization that permits the use of mobile devices has suffered some form of mobile attack, Check Point Software Technologies found in a survey last year of 850 organizations. While not all of the attacks resulted in actual security breaches, the data showed that organizations are under constant mobile attack.

David Gehringer, an analyst at Dimensional Research, says there has been a marked increase in the availability of malware for stealing VPN and other credentials for logging into enterprise networks and applications. Typical tactics have included SMS redirects and screen overlay attacks. Criminals increasingly are looking to use the information gained via these attacks to highjack user accounts and gain access to enterprise networks.

More recent attacks have begun leveraging some core capabilities of smartphones and tablets such as geolocation tracking, camera functions and application runtime environments to snoop on users and steal data, says Will LaSala, director of security solutions at VASCO Data Security. One example he points to is Skygofree, an extremely sophisticated Android tool developed by an Italian IT company for lawful intercept purposes that spies on conversations, text messages and photos, and features a never-before seen location-based audio recording capability.

Increasingly, attacks against mobile devices have begun targeting cryptocurrency wallets. A large number of malware attacks now also include hidden tools that steal a mobile device's processing capabilities for cryptocurrency mining, LaSala says.

Leaky applications, applications with over-reaching permissions and applications with unwanted functionality such as adware and hidden backdoors are other issues, especially for organizations that permit the use of unmanaged, personally owned mobile devices for work.

Users who download such applications can expose enterprise data to unforeseen risks. Until recently, such apps only posed a risk to users who downloaded applications from untrusted third-party sources. But over the last year, malware authors repeatedly managed to upload dodgy applications even into official app stores such as Google Play, significantly heightening risks for users in the process.

To reduce their exposure, organizations need to start treating mobile devices just like they do any other corporate computing asset on the network, says Pete Lindstrom, an analyst with IDC. "Over the past few years what we have seen is Android and iOS becoming just another operating system on just another device that is corporate-owned." The same precautions organizations put in place to protect against malware, malicious apps and abuse for their other endpoint assets need to be applied to mobile devices as well, he says.

Over the past few years what we have seen is Android and iOS becoming just another operating system on just another device that is corporate-owned."

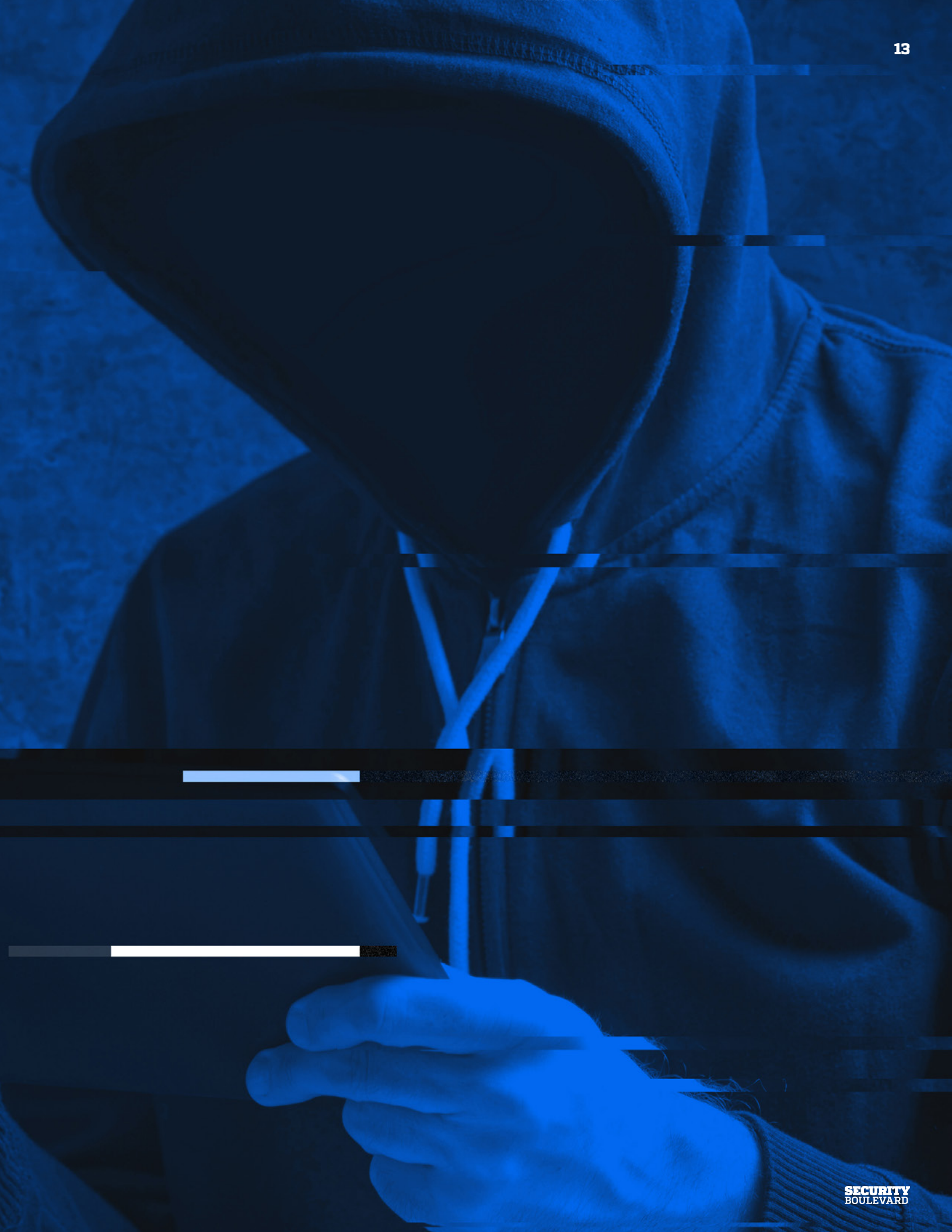
**– Pete Lindstrom
451 Group**

Conclusion


C yberattackers have managed to stay one step ahead of defenders by constantly evolving their tactics, techniques and procedures. They tend to use a particular tactic or technique only for as long as it works for them before moving on to something else. Ransomware and DDoS attacks are popular for the moment because attackers—or at least some of them—are profiting from these strategies, while IoT and mobile present more of an untapped opportunity. Inevitably, when organizations get better at addressing these threats, criminals will find other ways to attack.

For enterprises, the trend dictates a strategic rethink of their approach to security. Rather than seeking to eliminate every single threat and blocking every single attack, the focus has to be on managing cybersecurity risk in a manner that is cost-effective and aligns best with business interests.

As the National Institute of Standards and Technology (NIST) explains in its widely popular Cybersecurity Framework, properly mitigating cyber risk requires that organizations implement controls to identify, protect, detect, respond and recover from threats. A strategy focused on blocking threats at the network perimeter these days is simply not enough.



SECURITY BOULEVARD

 securityboulevard.com
 twitter.com/securityblvd
 facebook.com/secboulevard/