5 Major Security Threats and How to Stop Them

Successful security breaches—and even more attempted breaches—happen constantly across organizations of all sizes and industries. There are more types of attacks and more devices at risk today than ever. Phishing, hacking, credential theft and abuse, social engineering, denial of service, ransomware, and the use of backdoor or command-and-control (C2) malware all pose real threats.

The first nine months of 2019 saw 5,183 breaches globally, exposing 7.9 billion records—one-third more breaches and more than twice as many exposed records compared to the same period in 2018.[1] The reality is that when it comes to breaches, it's not if your organization will be hit; it's when.

The key to keeping your organization safe is knowing what types of threats exist and how you can stop them from having a major impact. This paper will look at five of the latest security threats and explain how Palo Alto Networks tools can help keep them from threatening your organization.

1. "Data Breach QuickView Report, 2019 Q3 trends," Risk Based Security, November 2019, https://pages.riskbasedsecurity.com/data-breach-quickview-report-2019-q3-trends.

1. Container Compromise

To test just how secure cloud native tools are, researchers from Palo Alto Networks created an application based on a published and ready-to-run Drupal 8 application. They used a full cloud native security buildout. The CI/CD pipeline used Git for source control management; Docker for container deployment; and Jenkins for building, testing, and deploying to AWS®. The container was compromised in 45 minutes.

The adversary used a built-in command within the container to execute a local script. Ultimately, the application fell victim to a Jenkins vulnerability—one of many—that allowed anonymous users to become administrators.[2] The Jenkins vulnerability allowed the adversary to run a script through Ngrok™ (more on this in the next section), further opening up any organization using the application to exploitation. From there, attackers could steal data, deploy ransomware, or even use the organization's server to launch an attack on another server. In this case, the malicious actors used their administrative control to mine cryptocurrency—a scheme detected by Palo Alto Networks Unit 42.

Cryptojacking malware called Graboid, originally discovered by Unit 42, spreads by using containers in the Docker engine. This makes Graboid difficult to detect because most endpoint protection software does not analyze data in Docker engine containers.

2. Public URLs Exposing Your Server

In the previously mentioned application test and breach, the adversary ran a script through Ngrok, a multiplatform tunneling reverse proxy application that establishes secure tunnels from public endpoints such as the internet to locally running network services, such as servers. This application bypasses security infrastructure and creates a tunnel brokered through the Ngrok server. Because Ngrok hosts within AWS, all you'll see is AWS-to-AWS traffic, when it's really the adversary hijacking your server.

It took just milliseconds for the adversary to run a script that fingerprinted the host and exfiltrated data, killed competing processes, pulled the payload, and executed. In a real-world setting, once the payload had been executed, open credentials could have been stolen, ransomware launched, or a phishing campaign initiated.

3. Virulent Malware

There are almost as many variants of malware as there are devices on the internet. Among them, the Emotet malware family may be the most virulent. Emotet is a modular banking Trojan so treacherous that the US Department of Homeland Security once described it as "the worst ever." Threats from this Trojan continue to grow, with heavy activity already detected in 2020.[3]

Emotet primarily acts as a "dropper," or a downloader of other malware. After infection, it can quickly spread to other systems in the network, download other malware, and reinfect a compromised system after removal. Emotet primarily spreads via malicious email attachments and attempts to proliferate within a network by brute-forcing user credentials and writing to shared drives. Emotet can evade signature-based detection and is intent on spreading itself, making it very difficult to combat.

An adversary could use an Emotet infection to obtain sensitive information, such as banking data, military data, and governmental information. Such an attack could result in the loss of proprietary information, reputational harm, and disruption of an organization's operations. More advanced groups also use Emotet to load up the TrickBot banking Trojan with the goal of dropping Ryuk ransomware on the infected system.

4. New Approaches to Phishing

In the world of breaches, phishing is nothing new, but phishing links within PDFs are becoming more problematic than ever. Instead of adding malicious links to an email that some email gateways can detect and quarantine, adversaries are embedding these links within PDF files. If a user opens such a PDF and clicks on one of the malicious links in it, they'll be directed to a fraudulent webpage that looks exactly like a real page the user might expect to see. Phishing links in PDFs are focused and specific, and they typically target an organization's login infrastructure. For example, a phishing link might redirect to a masked SSL URL that looks like the organization's Microsoft 365™ login page. These links are dangerous because they bypass legacy email protection solutions, leading users to assume they're safe.

Another trend involves credential phishing targeted at stealing victims' online banking information via multiple staged payloads. With this approach, an adversary may use a Word document with a macro that launches a JavaScript, which then launches multiple EXE files. Each of these payloads has a specific task, such as persistence, propagation, or stealing credentials. These multi-stage attacks can be difficult for individual security tools to detect and block, partly because some of the steps in such an attack may not seem malicious on their own, and partly because most tools can only see part of the malicious payload.

5. Domain Generation Algorithms

Domain generation algorithms (DGAs) allow an adversary to generate domains on the fly to deploy malware or a payload to an endpoint. The DGA technique is in use because malware that depends on a fixed domain or IP address is quickly blocked, which hinders operations. Rather than needing to be recoded or use a new server, the malware switches to a new domain at regular intervals. This allows it to avoid static DNS lists, which might otherwise detect and prevent the breach.

2. "Jenkins Flaw Can Allow Hackers to Log In as Admins," SecurityNow, December 19, 2018, https://www.securitynow.com/author.asp?section_id=649&doc_id=748385.
3. "Increased Emotet Malware Activity," US Department of Homeland Security, Cyber-Infrastructure, January 22, 2020, https://www.us-cert.gov/ncas/current-activity/2020/01/22/increased-emotet-malware-activity.

A predefined, static DNS list can be easily discovered with a strings command and avoided, allowing the adversary to successfully infiltrate the target network. C2 servers and ransomware routinely use DGA to seize control of an organization's systems, steal data, and hold the organization—and all its information—hostage.

How Palo Alto Networks Can Help Stop These Threats

Native security tools aren't enough to secure the cloud. Still, you can eliminate most threats if you have the right tools deployed across your environment. To prevent successful cyberattacks, you need to:

- See everything
- Reduce the attack surface
- Prevent known threats
- Prevent unknown threats

The Palo Alto Networks Security Operating Platform® offers tools to accomplish all these goals.

Next-Generation Firewalls

Your firewall serves as your first line of defense in any solid security platform. Palo Alto Networks Next-Generation Firewalls, in both physical and virtual forms, provide complete visibility across your network, with automated response capabilities to keep your organization safe. Start with a Next-Generation Firewall, and then accelerate your capabilities with cloud-delivered subscription services to lock down your enterprise security.

DNS Security

According to Palo Alto Networks Unit 42, almost 80% of malware uses DNS to initiate C2 procedures. It's impossible to keep up with the high volume of malicious domains, let alone advanced tactics like DNS tunneling.

Our DNS Security service uses machine learning to identify new malicious domains and quickly detect C2 or data theft hidden in DNS tunneling. DNS Security algorithms use historical and real-time shared threat intelligence to accurately detect tunneling behavior.

DNS Security expands the native ability of Next-Generation Firewalls to detect and prevent DNS tunneling. Protections are scalable and evasion-resistant, covering known and unknown variants of DNS tunneling. DNS tunneling is automatically stopped with easy-to-set policy actions on the Next-Generation Firewall and blocking of the parent domain for all customers. Because DNS Security uses Next-Generation Firewalls as sensors and enforcement points, it does not require any changes to your DNS infrastructure, and it sees all DNS traffic. As a result, it cannot be avoided by someone simply changing their DNS settings.

WildFire Malware Analysis

WildFire® malware prevention service automatically delivers protections based on shared, community-sourced threat data and advanced analysis, updated about every five minutes, to prevent successful cyberattacks. It stops advanced attacks with built-in evasion prevention using a custom hypervisor and bare metal analysis, with machine learning as well as static, dynamic, and other advanced analysis techniques to keep organizations ahead of attackers.

Following static analysis, WildFire delivers an immediate verdict, which eliminates the window for an adversary to succeed. It delivers a signature while analyzing a file dynamically to extract information, and then delivers rich reports. WildFire finds 75% of malware within seconds for supported file types.

In addition, WildFire performs recursive analysis, analyzing the initial payload and subsequent payloads independently. This approach forces adversaries to replace every phase of the attack lifecycle. SOC analysts receive reporting data for all phases, mapped with protections delivered.

URL Filtering

URL Filtering automatically prevents attacks that leverage the web as an attack vector, including phishing links in emails, phishing sites, HTTP-based (C2) attacks, malicious sites, and pages that carry exploit kits. It includes inline credential phishing detection to detect in real time when users transmit their corporate credentials to an external URL. Image recognition and machine-based deep learning help stop evasive phishing.

URL Filtering assigns multiple categories to URLs that classify a site's content, purpose, and safety. Every URL has up to four categories, including a risk category that indicates how likely a site is to expose the organization to threats. More granular URL categorization means organizations can move beyond a basic block-or-allow approach to web access. Instead, they can control how users interact with online content that, while necessary for business, may be more likely to be used as part of a cyberattack.

Threat Prevention

The Threat Prevention subscription includes intrusion prevention, network anti-malware, and C2 protections. Threat Prevention detects and prevents threats hidden in SSL-encrypted traffic and outsmarts polymorphic malware by focusing on payload instead of hash or filename. Signatures for all types of malware are generated directly from billions of samples Palo Alto Networks continuously collects, including from WildFire, our Unit 42 threat research, and third-party research and technology partners around the world. Protections are automatically delivered, on a regular update cycle, to Next-Generation Firewalls and the Threat Prevention service. Threats and indicators of compromise (IOCs) are easily correlated and reported on so your organization will know exactly who was compromised and how without having to dig through multiple logs.

Get the Protection You Need

Adversaries are getting more sophisticated, using automation, machine learning, and artificial intelligence to create more virulent ways to breach organizations' security. From container compromise to malware, social engineering, exposed servers, and domain generation algorithms, it can be hard to keep up. To reduce the attack surface, gain visibility across your network, and prevent known and unknown threats, you need unified, automated, sophisticated protection delivered in real time. With services like DNS Security, WildFire, URL Filtering, and Threat Prevention added to your Palo Alto Networks Next-Generation Firewall, you get the tools you need to block the latest threats—and those yet to come.

To stay up to date on emerging threats, check out the latest research from Unit 42.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com