VECTRA®

Five ways cybercriminals conceal command-and-control communications

Perils of the cybersecurity gap

A dangerous cybersecurity gap exists between the time an attacker successfully evades prevention security systems at the perimeter and the clean-up phase when an organization discovers that key assets have been stolen or destroyed.

Inside this gap, attackers have a huge advantage. They can easily outsmart prevention-based security defenses by employing complex and intelligently constructed attack methods, including concealing their attack communications in hidden tunnels, encrypted traffic and normal HTTP traffic.

Stealing valuable data is more complex than a smash-and-grab robbery. Modern cyber attackers are patient, strategic operators that infiltrate and stealthily persist in a network over an extended period of time. Think Ocean's Eleven rather than Bonnie and Clyde.

Cybercriminals move low and slow, taking an average of 146 days to carry out an attack, according to the 2016 Mandiant M-Trends report. To avoid detection, they make every attempt to conceal their attack communications as they move in closer to steal data.

Difficult to detect

Today's sophisticated attackers have the skills to evade perimeter security defenses, such as next-generation firewalls, intrusion prevention and detection systems, and malware sandboxes.

Once they are inside the network, attackers can operate from a position of trust. They can easily blend in with normal, trusted user traffic as they spy, spread and steal.

This means attackers now control both ends of the communication – the infected host inside the network as well as the external device or server from which a threat is launched.

Attackers who make their way into networks have greater flexibility to use or modify allowed applications, encrypt their communications and embed messages into seemingly ordinary traffic.

The attacker's success depends on the ability to spy, spread and steal without detection. And to do that, they employ a variety of covert communication techniques on their journey to find and steal critical assets.

#1: Encryption

Encryption protects communications from snooping, and it works well for good guys and bad guys. Bad guys can encrypt and hide their attack communications using a variety of methods ranging from standard SSL/TLS to customized encryption schemes.

Organizations rely on HTTP-based Web and cloud and software-as-a-service applications, such as Gmail, Box and Salesforce.com. These applications are increasingly encrypted, which safeguards legitimate content and simultaneously gives attackers a way to hide.

Some organizations decrypt outbound traffic for inspection but decryption causes a significant performance penalty because it can slow down the natural flow of business communications.

Privacy and regulatory concerns have emerged as one of the top barriers to inspecting encrypted traffic. For instance, HIPAA, FISMA, PCI DSS and Sarbanes-Oxley require that sensitive banking and healthcare traffic is not decrypted and inspected. Some countries have strict privacy laws that prohibit the inspection of encrypted traffic.

One of the most challenging aspects of SSL inspection involves certificate pinning, which is the process of associating a host or application with its expected certificate or public encryption key.

Many online services, such as Google, began to use pinning to deter attackers that use man-in-the-middle attacks on their Web sessions with valid private keys that could issue new certificates.

To validate a connection, pinning requires specific root certificates instead of a trusted certificate authority. Although this thwarts attackers with stolen valid certificates, it also breaks man-in-the-middle detection methods.

Attackers can additionally use their own encryption schemes by modifying existing encryption mechanisms or creating their own. Custom encryption is difficult to detect and virtually impossible to decrypt. This type of traffic easily bypasses prevention security systems without inspection.

#2: Hidden tunnels

Attackers use hidden tunnels for command-and-control and data exfiltration. Hidden tunnels are tough to detect because the communication is buried within multiple connections that use normal, commonly allowed protocols.

For example, attackers embed hidden malware requests in normal HTTP traffic, such as text fields, headers and cookies. So they're essentially hiding in plain sight within traffic that appears quite ordinary.

#3: Under cover in allowed applications

Attackers go to great lengths to blend in with everyday applications and emulate allowed application traffic. Their preferred hiding place is within the vast amounts of Web traffic in a typical enterprise.

They can emulate a Web browser to blend in and communicate with the outside world. Or they might use a fully automated browser and Web session to send and receive malware instructions to an infected device.

#4: External remote access

External remote access tools (RATs) enable attackers to exercise total, real-time control over infected devices and are typically used for targeted threats. With direct control, attackers can spy and spread laterally inside the network.

Like other hidden attack methods, RATs are hard to detect. Signatures exist for most known RATs. But attackers can modify existing RATs or create their own custom RATs to avoid detection and appear as Remote Desktop Protocol (RDP), Virtual Network Computing (VNC), WebEx and other common tools.

#5: Anonymizing technologies

Attackers use anonymizing technologies, such as The Onion Router (Tor), peer-to-peer (P2P) networks and other proxies, to obscure their true location and identity.

End users also use these tools to evade Web filtering and enterprise security controls. Either way, anonymization technologies introduce considerable risk to an organization.

With proxies, attackers or subversive users avoid URL and reputation controls. Because the communication is only with the proxy, the true final destination of the traffic is hidden.

P2P networks also provide a highly distributed layer of anonymity by routing traffic via a massive number of participating nodes. Attackers make extensive use of anonymizing technologies to hide the location of their command-and-control infrastructure.

Covert no more

Automated threat management models detect a wide range of hidden threats by using data science to mathematically analyze the subtle attack patterns within network traffic.

Today, automated threat management models are perhaps the best way to uncover underlying threat behaviors, such as command-and-control traffic disguised by encryption, hidden tunnels, allowed applications, RATs, and anonymizing networks.

To detect hidden tunnels, automated threat management models continuously monitor and analyze all traffic to reveal subtle anomalies, such as delays or abnormal patterns in requests and responses. These patterns can be detected using sophisticated data science techniques without decrypting traffic.

Together, data science, including supervised and unsupervised machine learning, reveal the presence of covert communications such as external RATs without depending on signatures, payload analysis or log analysis.

On the surface, the behavior of RATs may look like normal user traffic, but upon careful analysis, unique pauses within an open connection may indicate the presence of malicious attack behaviors.

For Tor anonymization networks, automated threat management analyzes traffic to identify its unique behavior patterns. The entry and exit nodes evolve constantly, and there are many separate, private Tor networks.

Regardless of the dynamics, focusing on behaviors will identify the presence of command-and-control communications. Similarly, by focusing on the behavior of P2P traffic, rather than the many variants of P2P software, hidden attack communications can be revealed.

Stopping bad behavior

Applying advanced data science models and machine learning algorithms reveals the true behavior and purpose of the traffic, finally putting an end to an attacker's considerable advantage.

With that power, security teams can pinpoint active cyber attacks while they're happening, correlate threats with the hosts under attack, and prioritize the attacks that pose the greatest business risk. Ultimately, they can quickly mitigate the threat and prevent data loss.

To learn more about the mechanics of covert attack communications and the various methodologies that can be used to expose them, download this white paper.

VECTRA®

Email info@vectranetworks.com **Phone** +1 408-326-2020 www.vectranetworks.com