Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 12, Issue 5

Funded Threats: The Fuel for Malware Evolution

By Nick Biasini, Craig Williams

The threat landscape is ever evolving, as our adversaries discover new ways of compromising systems. The monetization of hacking has had a drastic impact on the threat landscape. Today it is easier than ever for an adversary to monetize their nefarious activities. A couple of clear examples exist in Angler Exploit Kit and one of its favorite payloads, ransomware.

While threats like ransomware are steadily increasing due to increased profit and stealth, more traditional threats still exist for threat actors that fear no repercussions. The actors behind SSHPsychos are a great example of how old, well understood, vectors can still be dangerous when the threat actor seems to have little to no regard for stealth or operational security and no fear of reprisal.

In today's threat economy, there's tons of money to be made by compromising systems. With the growth of bitcoin and the adoption of anonymizing networks like Tor, adversaries are able to quickly gain access to their ill-gotten gains while still remaining largely anonymous without lots of middle men in the path. This allows the adversary to not only get money quickly, but also to monetize to the fullest extent without having to give portions away. We will spend a little time discussing each of these threats in detail, including how they have evolved over the last six months.

In order to protect networks and end users from today's threat actors, it is important for communications service providers to better understand the biggest threats in the last few months: the Angler Exploit Kit, ransomware, and the SSH Psychos.

Angler Exploit Kit

Earlier this year, Cisco singled out the Angler Exploit Kit as the one to watch among known exploit kits observed in the wild because of its innovative use of Flash, Java, Microsoft Internet Explorer, and Silverlight vulnerabilities. In 2015, Angler stands as the leader in exploit kit sophistication and effectiveness. The exploit kit's authors' recent concentration on, and quick work to take advantage of, vulnerabilities in Adobe Flash is an example of their commitment to innovation. On average, 40 percent of users who encounter an Angler Exploit Kit landing page on the web are compromised. This means

Angler can identify a known Flash (or other) vulnerability that it can exploit. It then downloads the payload to the user's machine.

Angler authors have also taken an interesting approach to the exploit kit's landing page. Historically these landing pages consisted largely of random strings of text. Angler authors have changed that drastically by incorporating text from Jane Austen's Sense and Sensibility into web landing pages. Adding passages of classic text to an exploit kit landing page is a more effective obfuscation technique than the traditional approach of using random text. Antivirus and other security solutions are more likely to categorize the web page as legitimate after "reading" such text.

Adversaries have employed two key strategies for driving users to the exploit kit: malvertising (malicious online advertising) and malicious iFrames embedded in random compromised websites. Together these strategies create a consistent stream of web traffic to these pages.

Evasion is a key differentiator in allowing Angler to compromise users effectively. "Domain shadowing" is one example of evasion techniques its authors have recently employed. Domain shadowing is a technique where exploit authors compromise a domain name registrant account to register a sub-domain under the legitimate domain to compromise users.

In addition to domain shadowing, the Angler Exploit Kit uses multiple IP addresses to make detection more difficult. The amount of IP addresses being used varies widely between a handful, less than five, to as many as 30 in a given day. Angler usually delivers an encrypted payload, which is often the ransomware variant, CryptoWall. If not initially blocked, this payload can be identified only retrospectively, and time to detection of the threat can take days.

Ransomware

In today's flourishing malware economy, cryptocurrencies like bitcoin and anonymization networks such as Tor are making it even easier for miscreants to enter the

malware market and quickly begin generating revenue.

To become even more profitable while continuing to avoid detection, operators of crimeware, like ransomware, are hiring and funding their own professional development teams to create new variants and tactics.

Ransomware encrypts users' files—targeting everything from financial files to family photos—and provides the keys for decryption only after users pay a "ransom".

Ransomware targets everyone from large companies to law enforcement to individual users. Ransomware is a multi-vector threat delivered to victims in nearly every possible way. All major exploit kits are now delivering some ransomware variant. Spam is also a common attack vector with a significant amount of spam campaigns leveraging attachments delivering ransomware variants such as CryptoWall, TeslaCrypt, and CTB-Locker.

The ransom demanded by these threat actors is not exorbitant. Usually, a payment between $300 and $500 is required to decrypt the files.

Why such a modest fee?

Adversaries who deploy ransomware have done their market research to determine the ideal price point. The idea is that the ransom is viewed by the victim as a "nuisance fee", and it will not make it worth their time to contact law enforcement. And users are paying up.

Recently, there have been a number of customized campaigns that were designed to compromise specific groups of users, such as online gamers. In addition, some ransomware authors have also created variants in uncommon languages like Icelandic to make sure that users in areas where those languages are predominantly spoken do not ignore the ransomware message.

Users can protect themselves from ransomware by backing up their most valuable files and keeping them isolated, or "air gapped" from the network. Users should also realize that their system could be at risk even after they pay a ransom and decrypt their files. Almost all ransomware is multi-vector. The malware may have been dropped by another piece of malware, which means the initial infection vector must still be resolved before the system can be considered clean.

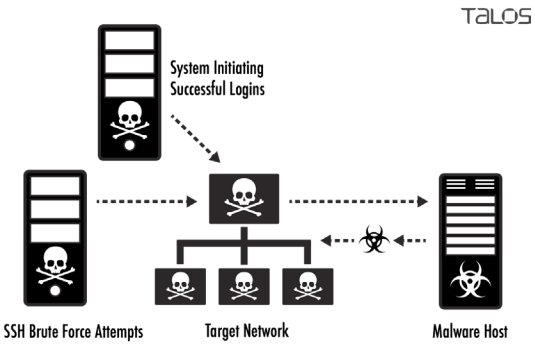
SSH Psychos

In June of 2014, our researchers identified a threat actor conducting a widespread brute force attack out of isolated networks in Hong Kong. A brute force attack is a large dictionary-based trial-and-error search of a key space using usernames and passwords. The threat actor used a dictionary of over 300,000 passwords, some of which were quite complex, in attempts to compromise the root account.

This threat actor gained special attention due to the sheer number of persistent and aggressive attacks.

Once the system was compromised, a separate network at a shared hosting provider in the United States would reach out to the system, login, and place a DDoS client on the machine.

This threat actor gained special attention due to the sheer number of persistent and aggressive attacks.

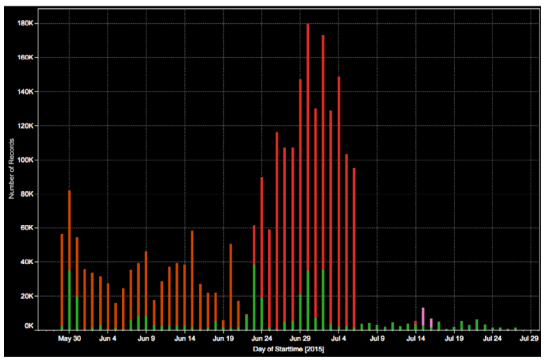


Our threat researchers collaborated with Level-3 Communications and was able to determine this threat was responsible for a third of the Internet's backbone traffic for SSH.

Normally a few machines with a DDoS client installed is not a very big concern; but, given the size of this brute force attack, there were likely tens of thousands of compromised machines now under the control of the threat actor.

This type of attack is very common, but it is rarely taken to these absurd lengths since it is so easy to spot. At this massive of a scale this DDoS network was a threat to large companies and even major portions of the Internet.

To combat this threat, our threat researchers, Level-3 and other communications service providers began blocking the actors' infrastructure on the Internet backbone. The threat actor attempted to migrate networks to avoid these blocks; but, due to the implementation of their network and the nature of the attack, they continued to be easy to spot. As of early July, the threat actor appears to have relented.



Conclusion

As the number of people and devices connected to the Internet increases, so does the financial gain for cyber criminals through their nefarious activity. This explosion in revenue, coupled with the adoption of bitcoin and anonymizing traffic protocols (Tor & I2P), have made for an evolving threat landscape.

Today, these threats are backed with large development efforts and are designed to compromise users delivering money to their creators quickly and effectively. While there are still more classic threats like SSH Psychos operating, this new group of threats designed for monetization is quickly growing and morphing, accounting for a larger portion of the threat landscape every day.

In the coming months, threats are destined to continue, evolve and expand; and it is up to communications service providers, as well as end users, to remain informed and vigilant in order to protect themselves – and their customers – from attacks on individuals as well as broader networks.

As the number of people and devices connected to the Internet increases, so does the financial gain for cyber criminals through their nefarious activity.