Infocyte®

Financial Infrastructure Top Malware Target

Hunt Financial Malware with Infocyte

ISTR Findings of Note:

- 1.2 million instances of financial malware attacks
- Number of Ramnit detections was approximately equal to all ransomware detections
- Three threat families were responsible for 86% of all financial threat attacks in 2016:
  - Ramnit (38%), Bebloh (25%), and Zeus (23%)
- Three most infected countries: Japan, China, and India
- Lazarus attacks in 2016 were the first time there was strong indications of state involvement in financial cyber crime
- APT groups are using financial malware to blend in with more common attacks

> "When it comes to attack trends, we are seeing a much higher degree of sophistication than ever before. While nation-states continue to set a high bar for sophisticated cyber attacks, some financial threat actors have caught up to the point where we no longer see the line separating the two. Financial attackers have improved their tactics, techniques and procedures (TTPs) to the point where they have become difficult to detect and challenging to investigate and remediate."
>
> - Mandiant M Trends Report 2017

Financial Malware More Prevalent Than Ransomware

While headlines and news coverage leave the impression that ransomware is the greatest threat to enterprises today, research has revealed that with annual attacks numbering 1.2 million, financial malware is **2.5 times as prevalent** as ransomware.

The recently released Symantec Internet Security Threat Report (ISTR) Financial Threats Review 2017 stated that 38% of all financial threat detections were against corporations, rather than customers. While these attacks are more difficult to execute, they yield a higher profit, which is why there was 1.2 million such attacks in 2016.

Attacks against financial institutions are on the rise, with the emergence of a select group of cyber criminals targeting financial institutions in a sophisticated manner. Incidents targeting banks have spread around the world, striking institutions in Ukraine, Poland, Bangladesh, Ecuador, U.K. and India, to name a few, with losses totaling hundreds of millions of dollars. These widespread events indicate that financial criminals see these networks as prime targets for attack.

Attacks Are Varied

From financial Trojans that attack online banking, to attacks against ATMs and POS machines, there are a variety of attacks uniquely targeted to elements of the financial infrastructure.

In some cases, attacks against financial institutions do not directly attempt fraudulent transactions. In these cases, attackers attempt to profit from the break-ins by selling stolen information, profiting from insider trading on gained information or blackmailing the banks.

For example, in November 2016 newspapers reported on a case of a bank in Lichtenstein where cyber criminals had breached the bank's security measures and extracted the account information of various customers. Subsequently the customers received a blackmail notice demanding they pay 10 percent of their account balance or risk having their information published online.

These incidents, along with past attacker activity, indicate that many attackers are increasingly focusing on corporate targets, whether the financial departments of corporations or financial institutions themselves.

Geographical Shift

2016 also saw a geographic shift in successful infection rates, specifically a big increase in Asia. Japan now holds top spot for the most financial malware infections, jumping from 3% of global infections to 37% in one year[1]. China and India also now appear in the top 10 list of countries targeted by financial Trojans, indicating that attackers are targeting markets that are less saturated and less protected.

The trend is projected to continue, with predictable results. Financial institutions in markets such as Africa, the Middle East and Asia must prepare for an increase in the volume and sophistication of malware attacks and infections.

[1] Symantec Financial Threats Review 2017

Ripped From The Headlines

Some recent high profile attacks on financial institutions demonstrate how devastatingly effective malware can be, and how inadequately prepared many financial organizations are.

February 2017: Organizations in 31 countries, including many banks, were hacked using malware that was unwittingly distributed by the KNF, the Polish financial regulator, which is how the malware disguised itself as 'trusted' and gained widespread dissemination. This attack began in late 2016 and was detected in early February the following year.

March 2016: Buhtrap attacks endpoints at a number of Russian banks, compromising machines with malware that had evasion techniques, as well as the capability to take screenshots, keystrokes, and other intelligence. This was a long running hack, between August 2015 and February 2016 the malware resided undetected. At one point over this time period, attackers started using a worm, dubbed 'BuhtrapWorm', which allowed attackers to remain in the targeted corporate network as long as at least one computer was infected. The resulting losses amounted to approximately $25 million USD by the time the theft came to light.

February 2015: From 2013 onwards, Carbanak targets over 100 banks and other financial institutions in 30 countries. Attackers use a stolen security certificate to evade defenses, leveraging the organizational trust in vendor certificates to gain access and deliver the malware payload. The malicious program lurked for months capturing everything from keystrokes to video feeds, equipping the attackers with the right information to impersonate bank officers, turn on ATMs and transfer milions of dollars to dummy accounts. The estimated cost of this hack is $300 million USD at minimum, possibly three times that amount.

Hunt Malware and Protect Enterprise Assets

Infocyte HUNT™ offers financial institutions the ability to proactively and iteratively hunt malware and other persistent threats that have evaded defenses and reside undetected. A common repeating theme that contributes greatly to the utlimate financial cost of these hacks is the lengthy dwell time, the period of time that malware is allowed to persist undetected and continue to wreak havoc and do damage.

The Forensic State Analysis (FSA) approach used by Infocyte HUNT enables an organization to schedule regular scans of endpoints to find any cases of suspicious activity. There is no need to wait for a high profile event, such as theft being detected, to call attention to the breach and precipitate discovery.

For example, a bank can decide that a 12-hour window is the acceptable breach discovery window to risk malware residing undetected on their endpoints: workstations, servers and ATMs. Infocyte HUNT then scans the endpoints regularly at 12 hour intervals to validate endpoints.

In addition, Infocyte HUNT dispels any superficial trust in security vendors, solutions, and even business partners - removing the ability to exploit such trust. The source of a file is irrelevant, Infocyte HUNT finds **anything** suspicious.

Infocyte HUNT

- Definitively answers if you have been breached
- Advanced detection combines forensic automation and patent-pending memory analysis
- Infocyte's platform uses volatile memory analysis to reconstruct the state of an endpoint at a given point in time
- Infocyte HUNT is not reliant on a host OS, which may be itself compromised
- Fast. Infocyte HUNT can scan upwards of 50,000 endpoints per day
- No training required to effectively use Infocyte HUNT
- Final report provides actionable intelligence within minutes

Start Hunting.
Contact us to learn how.

Infocyte®

CORPORATE HEADQUARTERS
110 E. Houston St. Floor 6
San Antonio, TX 78205
+ 1.844.INFOCYTE (844.463.6298)
sales@infocyte.com

www.infocyte.com
@InfocyteInc