Cybersecurity in the Financial Sector

2017 Review - Looking ahead to 2018

WHITE PAPER

Infocyte®

Table of Contents

Executive Summary

For any financial services institution, right now one of the top of mind concerns must be cybersecurity. Institutions, from banks to investment houses to insurance companies, all want to protect themselves from the widening range of malicious actors targeting them. While the threat landscape for the Financial sector continues to both evolve and to become more dangerous, what is required is a shift in mindset when approaching cybersecurity. The sector is exposed to unique threats, and old fashioned ways of thinking about security are no longer sufficient.

2017 has seen massive cyberattacks hit major institutions worldwide. Also notable, there was a shift in the types of attacks targeting financial entities. The threat landscape for the industry shifted from events caused primarily by internal actors to those caused by someone external to the company.[1]

The rate of financial malware has been increasing for some time. According to Symantec's *Internet Security Threat Report: Financial Threats Review 2017* the proportion of threat detections in the industry targeting corporations rose to 38% in 2016. These attacks are admittedly more difficult to execute, however they yield a higher profit, which is why there was 1.2 million such attacks in last year. Once the numbers are in for the current year, it is likely that the attack number for 2017 will be even higher.

Some other trends that were witnessed this year include:

- The continued domination of banking Trojan malware. At the time of this writing the Ursnif/Gozi banking Trojan, after attacking European targets in Spain, Poland, Bulgaria and the Czech Republic earlier this year, is currently amplifying attacks on Japanese banks and payment card providers.
- The extensive penetration, in up to 40 countries, of financial malware such as Dridex and Trickbot. Certain older malware families are increasing in activity, such as Ramnit, while newer codes are slowly but steadily increasing their reach and spread, such as Gootkit and Qadars. Zeus maintains its position as the leading malware Trojan.
- Tailored malware written to specifically exploit weaknesses in a given institution's processes or defences. Given the nature of banks and financial institutions, details on such tailored customised malware is rarely made public, but our experience in the market has indicated that virtually everyone has stores and collections of discovered samples residing with their incident response and/or SOC teams.
- Attacks on ATM/POS systems. Previously ATMs were primarily at risk from malware that required physical access to the machine. This year, a new trend emerged where attacks on ATMs were conducted over the enterprise network. POS systems have continued to come under malware attacks which are notable for the lengthy dwell times, where malware resided undetected for long periods of time, significantly increasing the damage and cost to customers.
- The proliferation of criminal tools on the Web has made executing attacks affordable. Practically anything is now accessible for a price. Malware as both a product and as a service is for sale in the online criminal marketplace. Basic malware is going for as little as $1, with password stealers selling for $50, and RATs costing $200. Services offered include hacking of email accounts and CMS websites, and the installation malware and malicious file encryption.[2]

Ursnif (aka Gozi) banking Trojan

Ursnif was the most active malware code in the financial sector in 2016; both it and its derivatives have continued to plague banks throughout 2017.

Hackers have been leveraging Ursnif against North Korea, Europe, Australia and Japan for years. This year, Ursnif has targeted banks in North America, Australia, Japan, Spain, Poland, Bulgaria and the Czech Republic.

Since September 2017 Ursnif attacks against Japanese banks and payment card providers have amplified.

The Ursnif malware configurations currently targeting Japan are specific to banks and payment card providers in the country. To deliver the malicious Ursnif payload in Japan, hackers use fake attachments claiming to be from Japanese financial services and payment card providers.

In other regions such as the UK, the attacks have used the RIG exploit kit to infect users through malvertising, which are online ads that incorporate or install malware.

[1] A Tale of an Industry: The Finance Sector & Data Breach Type Trends, Bitsight, October 2017
[2] A Hacker's Tool Kit, Fortune Magazine, October 2017. Source data from Recorded Future.

The combination of these factors and trends has made the financial sector the target of unique threats, and at an unprecedented scale.

The pressure continues to increase; successful attacks result in asset losses, reputational damage, angry and upset customers, higher cyber insurance premiums, displeased shareholders and irate board members.

So let's take a closer look at the fundamentals at work in this scenario. Conceptually, when it comes to security, it is important to examine both the predicating beliefs common in an industry, and the behaviours they encourage.

Beliefs and Implications

If a bank is functioning under the BELIEF that defence equals security, and that defences are infallible, it will eventually fall victim to cyber threats. The implications of this belief are demonstrated in an over-reliance on defences, where the general mentality is that X amount of dollars has been spent on defensive products, and different types of defensive tools have been layered, thereby achieving the maximum security possible.

Implications of any belief are expressed in behaviours. Behaviours are only good or bad in the context of achieving some result.

In the context of achieving stronger cybersecurity, one can operate with an unuseful belief, such as:

- Trust that threats are adequately countered with defensive measures

Leading to behaviours where a bank:

» Depends on defences to protect enterprise assets
» Operates with the understanding that 'no news is good news', i.e. is prepared to fly blind, with no ability to demonstrate that assets are safe

On the other hand, a company can operate with a useful belief, that:

- Understands that malware will breach defences, no matter what they are

Leading to behaviours where a bank:

» Accepts that utilizing tools to hunt this malware in a small window of time is the best case scenario
» Adopts the capabilities to hunt malware and APTs residing undetected, i.e. is prepared to validate their endpoints compromise status on demand, and can obtain this information at will

If a bank takes a proactive stance – and builds in a hunt program – it is armed and equipped with the tools required to protect assets.

The malware targeting the industry today is so virulent and dangerous that it poses the risk of destroying the fundamental infrastructures, whether virtual or physical, that organizations depend on.

Not all software investments in the industry are viewed as operational costs. Platforms such as core banking, treasury, and trades management are all understood to be integral and essential to the fundamental business goal, which is to generate profit.

As such, these banking platforms are not viewed as short term, commoditised, purchases. Rather they are viewed as long term, mission critical, investments that will yield returns.

[3] Phishing Activity Trends Report: 1st Half 2017, Anti Phishing Working Group ,October 2017

FINANCIAL MALWARE DEFINED:

Financial malware describes the emerging trend of using specialized malware, which has been built to scan a computer machine or an entire computer network, to gain information associated with financial transactions.

Financial malware is employed by hackers to commit banking fraud cybercrimes. Considered one of the newer types of cybercrime, financial malware has managed to bypass secure information technologies developed specifically to protect the monetary assets of financial institutions and their customers.

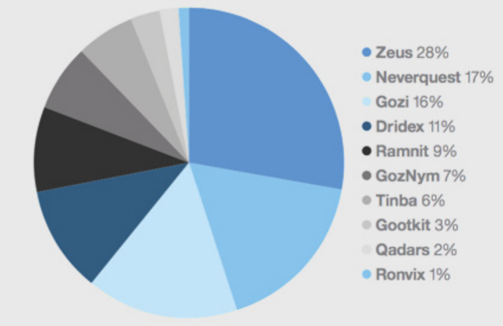
The Anti-Phishing Working Group (APWG) has released its 2017 H1 report[3]. The findings state that phishing attacks on Financial institutions account for 26% of incidents. The Payment industry accounts for a full 45% of attacks. Taken together these figures mean that 71% of attacks targeted enterprises in the financial sector.

THE TWO FORMS OF FINANCIAL MALWARE ATTACKS:

General Attacks: This type of malware is developed to steal the login information of the user not only for banking sites, but also for any secure socket layer sessions. For instance, these types of attacks also grab credentials for social networking sites and Web-based emails.

Targeted Attacks: This kind of attack made the Zeus malware famous. The attacker intentionally creates configuration files for particular online financial organizations. Then, the attackers make use of these files to trigger the man-in-the-browser (MitB) attack, which is a technique in which the configuration file provides a fake Web page to the Internet browser.

TOP 10 BANKING TROJANS FOR 2017[4]



[4] Data from IBM XForce "The Shifting Panorama of Global Financial Cyber-crime", 2017

SWIFT Related Malware Heists

- Far Eastern International Bank Taiwan: malware planted on servers and SWIFT terminal enables hackers to steal $60 million.
- $81 million stolen from Bangladesh Central Bank.
- $12 million stolen from Banco del Austro (BDA) in Ecuador.

ATM/POS Malware

- Hitachi Payment Systems machines successfully attacked, affecting 3.2 million debit card transactions.
- Trump Hotels: POS systems compromised at seven hotels in Chicago, Honolulu, New York, Toronto, Las Vegas, and Miami. Breach lasted for over one year.
- International Hotels Group: POS systems infected at over 1,200 locations. Breach lasted for over 6 months.
- Eddie Bauer: POS systems compromised at 360 locations for over 6 months.

SECURITY IS A BUSINESS DECISION

It is time that security related purchases are viewed through the same lens – as critical investments that yield returns. A failure to adopt this view effectively equates to an institution willingly accepting unnecessary risk.

Conversely, an institution that understands that the capability to hunt malware and APTs lurking undetected on endpoints is as crucial and critical to core operations as its revenue generating platforms is an institution that is approaching today's cybersecurity in a mature fashion, with open eyes maintaining dutiful vigilance.

When decisions to invest in cybersecurity are being made, representatives from the business must be involved in the selection process. The security of enterprise assets is no longer just an IT job, it's of crucial importance to the enterprise at large. As such, business needs to be at the table to fully understand the implications and the value in question.

Industry Values

Financial institutions of all kinds operate with similar values. Some common core values include:

- ◊ Integrity
- ◊ Teamwork
- ◊ Excellence
- ◊ Commitment
- ◊ Honesty

How can these values be respected and lived when any assurance of security is predicated on a dated belief that is no longer useful?

Reliance on defences, when the reality demonstrates that defences fail, erodes the integrity of the consumer contract, the trust that customers place in a bank to keep their hard earned cash and investments safe.

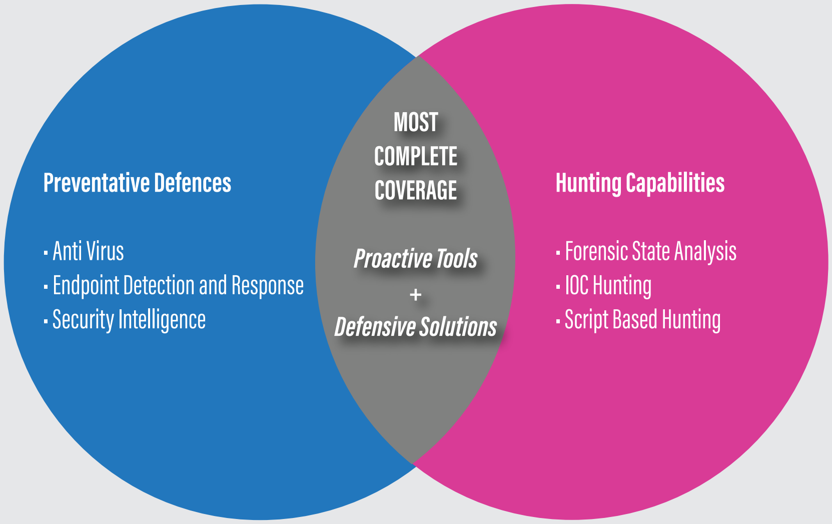
This same dated belief corrupts teamwork. Any integrated enterprise is comprised of different departments working together to achieve a shared goal. When there are unknown threats lurking within an enterprise, these often execute laterally. One wave of malware can seed secondary threats, and infection is transmitted through network connectivity.

Excellence and commitment both are equally difficult to maintain, when an attacker has successfully contaminated systems, siphoned funds, gathered intelligence, and more. Last, but not least, we have honesty. As guardians of wealth and traditionally representative of trust itself, it is imperative for financial institutions to take any and all steps necessary to secure assets. Institutions that do so can honestly assure their customers that security is a priority and advanced measures to ensure it are taken.

There are many other core values that financial institutions espouse such as respect, service, professionalism, community, trust, and loyalty. Each one of these key values is affirmed by institutions when they adapt and modernise their approach to security to reflect the current cybersecurity landscape.

For a financial institution to live its values in reality, it must adapt both its belief system about cybersecurity, and its corresponding behaviours to mirror this updated belief. It takes both offence and defence to adequately meet today's security challenges.

Both Defence and Offence are required to deliver robust security.



Modern Approaches to Cyber Security

Adopting this new approach to security can, and should, be done in several ways. One element is defensive, and one focuses on post breach detection. It is virtually impossible to accomplish robust security without engaging in both defensive and proactive measures.

Defence or Offence

Modern defensive measures include the adoption of endpoint detection and response (EDR), security intelligence (SI), and network and endpoint behavioural analytics.

Defence has come a long way from firewalls, AV and whitelisting. Today's bleeding edge defensive solutions are highly effective at monitoring activity and behaviours both on endpoints and across networks.

These solutions are effective in preventing threats from breaching enterprise assets and securing a foothold in the estate. However, none of these defences, even when layered and combined, delivers complete and total security and safety from threats.

Some malware successfully breaches defences and resides undetected, often for long periods of time. It is this malware that poses one of the greatest dangers for enterprises today. It poses this danger precisely because so many are labouring under the mistaken belief that security is defensive by nature. Such companies purchase defensive solutions, deploy them and then proceed to function believing themselves well protected and secure.

The defensive solutions that allowed the malware to breach cannot be trusted to hunt this same malware down after the fact.

To accomplish this, the second element required for strong security is post breach detection. Post breach detection is essentially hunting for malware and APTs that have breached defences and are dwelling undiscovered.

Post Breach Detection is Mission Critical

Solutions that offer post breach detection should be viewed in the same way as other mission critical investments like trading platforms. These are tools that allow enterprises to manage their dwell time and maintain consistent control over the threat that malware poses.

Post Breach Detection can be achieved today using one of four methods.

Script based hunting

There are several open-source platforms on the market that have well developed hunt methodologies. Generally speaking, script based hunting solutions provide a collection of tools that administrators and it security professionals can use to quickly survey endpoints and enrich collected data using a mix of third-party commercial and open source tools. These solutions are a good starting point for technical resources to begin forensic work.

Indication of Compromise (IOC) Hunting

Hunting based on IOCs involves searching through log files, looking for typical attacker tools and anomalies in user accounts and sessions, examining error reports, dump files, network connections and more. This approach can be effective and is suitable for adoption in organisations with highly skilled technical resources that can manage and maintain the solution and the feeds required to operate it.

Incident Response Solutions repurposed to hunt

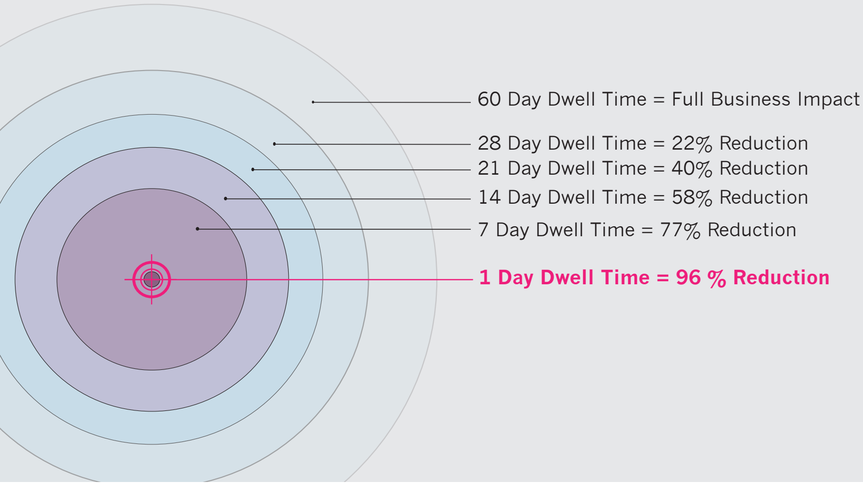
There are a number of digital forensics and incident response solutions available in the market. The challenge inherent in repurposing these tools to hunt malware is that they do not scale and also require highly skilled examiners to operate. This approach may be effective for small enterprises who decide to employ key expert personnel or who outsource the work of hunting.

Forensic State Analysis Hunting (FSA)

There is a single solution on the market today that delivers forensic state analysis – it is Infocyte HUNT™. FSA is an automated approach to post breach detection that assumes devices are already compromised and seeks to validate every endpoint as thoroughly as possible. The automation inherent in FSA enables users to effectively deploy rapidly, dynamically, and at scale.

FSA operates independently from the host OS and uses dissolvable endpoint surveys to quickly collect live forensic data from both volatile and non-volatile memory. Non-memory based information is also collected to identify persistence mechanisms. This data is then analyzed using a variety of post-breach analytics techniques, reputational, and multiple threat intelligence sources. Combining this live host forensic data and these analytic techniques, FSA determines the compromise state of endpoints.

Research[5] produced for Dell SecureWorks has indicated that organizations that limit their dwell time to 7 days realize a reduction in business impact of 77%. Further reducing dwell time to 1 day delivers a reduction in business impact of 96%. These are significant impacts when read through the lens of asset values under management in the financial industry at large.


60 Day Dwell Time = Full Business Impact
28 Day Dwell Time = 22% Reduction
21 Day Dwell Time = 40% Reduction
14 Day Dwell Time = 58% Reduction
7 Day Dwell Time = 77% Reduction
1 Day Dwell Time = 96 % Reduction

Infocyte HUNT:

- Definitively answers if you have been breached
- Advanced detection combines forensic automation and patent-pending memory analysis
- Uses volatile memory analysis to reconstruct the state of an endpoint at a given point in time
- Is not reliant on a host OS, which may be itself compromised
- Is fast. Infocyte HUNT can scan up to 50,000 endpoints per day

Post Breach Detection with Infocyte HUNT

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 ultimate 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 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.

[5] Quantifying the Value of Time in Cyber-Threat Detection and Response, Aberdeen Group, February 2016

Forecast 2018

Cyberattacks will continue to increase, both in the financial sector and in other prime targets such as health care and government. In all cases, cybercriminals will seek to monetize their attacks. As such, this activity will often touch financial institutions, which will continue to bear the brunt of monetary losses associated with cybercrime regardless of the originally targeted industry.

Further, we can expect to see a rise in mobile and cloud-based attacks as these technologies gain consumer adoption.

Looking ahead, institutions should brace for increasing numbers of tailored attacks. Each round of tailored attacks will improve their effectiveness, leading to success in breaching core platforms leading to concrete damage to the institution. For example, an attack that successfully breaches an enterprise and extracts information from the trades management platform can expose vulnerabilities, creating opportunities for an actor to short the bank's positions. These are risks that have the potential to cause losses that will run into the tens if not hundreds of millions of dollars.

The industry will also witness an increase in the attacks on downstream processing entities that support banking operations. For example, companies that execute back end processing of electronic fund transfers are prime targets for attackers. In organisations such as these, malware can be designed to siphon off incremental amounts from each transaction, numbering in the tens or hundreds of thousands of transaction thefts per day. At the same time, this type of malware can be used to manipulate ledgers to delay detection.

The current trend in ATM and POS attacks will continue to develop, malware will mature as will delivery techniques, requiring less physical access to compromise the machines. This will enable a greater scope to attacks and a greater level of coordination and sophistication with less risk of detection for perpetrators.

Change the Culture for Results

As has become normal, the business of cybercrime will continue to keep pace with technical evolution.

A paradigm shift in how cybersecurity is understood in the financial industry is required. Making this shift is a necessary step that will enable both effective preventative defence and productive proactive offence in countering the threat posed by malware today.

Adopting post breach detection capabilities is essential moving forward. Organisations with these capabilities have a proactive safety net that should become part and parcel of the enterprise, considered as integral and critical as key platforms.

Ideally, hunt programs will become part of the fabric and culture of the modern financial enterprise. These are iterative processes that should be conducted with regular frequency. How frequently will depend upon the speed and scalability of the post breach detection platform chosen. Platforms that offer users the ability to hunt for malware should be viewed as investments similar to those made in fundamental baseline platforms that generate revenue, rather than as defensive software tools.

Financial institutions who fail to adopt malware hunting capabilities will put at risk their institutions' ability to conduct business – attackers only have to succeed once in order to do damage, and they're getting better all the time.

Infocyte®

About Infocyte

Developed by former US Air Force cybersecurity officers, Infocyte's hunt technology fills a void left by today's real-time detection solutions. By focusing on the post-compromise activity of persistent attackers and insider threats, Infocyte's unique approach to security helps organizations defend their networks and critical information.

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