2015 INDUSTRY DRILL-DOWN REPORT

FINANCIAL SERVICES

Copyright © 2015 Raytheon Company.

Raytheon | websense

OVERVIEW

"It is one of the security risks that I would place very near the top of the things that the financial sector needs to work on…it's something that regulators, governments and the banks should put a lot of resources into."

- Former Federal Reserve Chairman Ben Bernanke on cybersecurity; June 2, 2015 (i)

Increasingly, cybersecurity is a primary focus for businesses of all sizes in every industry, but no more so than for the financial services sector. Today, financial leaders and authorities are acutely aware of the financial sector's status and vulnerability as a major target of cyber-attacks. No less than 80 percent of leaders in the banking and financial services sector cite cyber risks as a top concern, according to 'The 2015 Travelers Business Risk Index' (ii). Furthermore, the Identity Theft Resource Center has already tallied 30 known breaches in the Banking/Credit/Financial sector in the first half of 2015 alone. (iii) Significantly, the Financial Stability Oversight Council, which is charged with identifying risks to U.S. financial stability, highlighted cyber-attacks as "a growing operational risk to the financial sector" in its 2015 Annual Report. (iv) And, according to the 2015 Makovsky Wall Street Reputation Study, 83 percent of financial services firms cite defending against cyber threats and protecting personal data as one of their biggest challenges in building or maintaining their reputation over the next year. (v) Clearly, defending the financial sector against cyber-attacks is a top-tier priority.

The concerns cited in the studies above (and in Chairman Bernanke's statement) underscore the critical importance of cybersecurity to the financial industry and to society as a whole. The banking/financial sector – which includes the capital and equity markets - is the source of almost all capital flows upon which societies and business activities around the world depend. And because the free flow of capital is crucial for both the financial system and the financial industry to function properly, trillions of dollars must be in motion every day. The potential damage and disruption to these markets from a successful data breach is almost incalculable, but includes loss of revenue and consumer confidence, reduced profitability, reputational damage, higher debt levels and currency devaluations, among other risks. Willis Group Holdings plc, a leading global risk advisor, insurance and reinsurance broker noted in an April, 2015 report that "Given the interconnectivity of the internet, today's rapid digital advances and social media platform, a cyber crisis at one or more banks can result in financial catastrophe, not only to customers and banks, but to the country's financial system as a whole." (vi)

Copyright © 2015 Raytheon Company.

There is little wonder the financial sector is a prime target for cybercriminals; banks and financial institutions are truly where the money is. Regardless of whether the motivation is financial gain, geopolitical, or a combination, threat actors have greater access to hacking tools and potential sponsors than ever before.

All of these factors have led to an explosion of highly sophisticated cyber-attacks against the financial sector. In fact, the financial sector was one of the first targeted by industry-specific cyber-attack techniques. Preventing data theft in this sector is of utmost importance for all financial institutions and governments invested in the integrity of the international financial system.

While it is assumed that financial services are on the forefront of cybersecurity adoption, other than a few stray headlines, there has been very little public information about what they need to protect against. How severe, how complex, how often are financial services targeted with cybersecurity attacks?

For the first time in history, the top attack methodology, techniques and malware families are all documented from real world feeds from finance businesses. This research details the latest security threats and types of attacks facing the industry today. By comparing industries, Websense has gained new insight into the attack patterns against the financial services sector.

FINDINGS

This report identifies the cyber threats and tactics targeting the financial sector, their effectiveness and the respective volumes of those attack techniques from January through May 2015. By comparing cyber-attack data across the industry, Websense Labs has gained several unique and specific insights into the attack patterns directed toward the financial services sector.

THE TOP SIX FINDINGS INCLUDE:

1. Financial Services Encounters Security Incidents 300 Percent More Frequently Than Other Industries
2. Thirty-three Percent of All Lure Stage Attacks Target Financial Services
3. Credential Stealing Attacks Set Sights on Banking
4. Fraudsters Switch-up Campaigns Frequently to Outfox Banking Security Measures
5. Financial Services Ranks Third for Targeted Typosquatting
6. Evidence Increasingly Suggests the Need for Global Economy Continuity and Cyber Insurance May be Hindering Real Security Adoption in Financial Services.

Copyright © 2015 Raytheon Company.

1 FINANCIAL SERVICES ENCOUNTERS SECURITY INCIDENTS 300 PERCENT MORE FREQUENTLY THAN OTHER INDUSTRIES

Under constant barrage by cybercriminals, the number of attacks against the finance sector dwarfs the average volume of attacks against other industries by a 3:1 ratio. Further, the sophistication and persistent nature of the attacks continues to challenge security professionals.

» Based on Websense Security Labs telemetry data from the Websense ThreatSeeker Intelligence Cloud and the Websense Advanced Classification Engine, the financial services (FS) industry is disproportionately targeted when compared to other industries.

» By analyzing the total number of security incidents across all industries, the volume of incidents within the finance sector and our installation base we can ascertain that:

» *On average, financial services businesses are attacked 300 percent more than other industries.*

2 THIRTY-THREE PERCENT OF ALL LURE STAGE ATTACKS TARGET FINANCIAL SERVICES

This means that hackers are spending a huge amount of energy targeting the finance sector with a disproportionate amount of reconnaissance and lures being devised in search of the big payload.

» *Due to the tremendous value at stake from compromising hosts in financial services*, criminals spend a tremendous amount of time on the reconnaissance and lure stages of attacks, both in variety and sheer volume of attempts.

» In targeted attacks, *the most common subject line and content matter in email lures tend to be professional in nature* and most frequently involve specifics around invoices, ACH and BACS payments and third-party vendors.

» *Once on, attackers want to stay on and get more info.* With 6.6 percent of all call home incidents, the evidence is high that once established on a host in financial services, cybercriminals are making distinct attempts to leverage the position by reaching out for additional instructions.

» This is born out in the metrics looking at the percentage of attacks on financial services as a percentage of global incidents:

STAGE (web)	% of Global Figure*
Lure	33.3%
Redirect	0.02%
Exploit Kit	0.6%
Dropper File	0.1%
Call Home	6.6%
Data Theft	n/a

**For full year 2014*

Copyright © 2015 Raytheon Company.

3 CREDENTIAL STEALING ATTACKS SET SIGHTS ON FINANCE

» As one would expect with financial services, data theft and credential stealing attacks are paramount to the attackers. When analyzing the top threats facing this industry, researchers noted that most had some data and credential-stealing elements. By volume, the top threats seen in the finance sector include:

Rerdom 30% | Vawtrack 13% | SearchProtect 13% | BrowseFox 4%

» Interestingly, the Geodo malware, with its own credential-stealing email worm, is seen 400 percent more often in the finance sector than other industries.

Rerdom

- Rerdom is affiliated with the most advanced versions of the Asprox family of malware. Asprox is responsible for a huge amount of attacks against every industry, with overall usage rates surging since June 2014.
- This attack group is often known as a spam generator, but it has vast functionality and is increasingly being used to target financial services customers.
- Malware activities include spamming, sending malicious emails, click fraud, harvesting FTP, browser, and email credentials, downloading additional malware, and searching for website vulnerabilities that can be exploited to infect new servers.

Vawtrack

- Vawtrak (also known as Neverquest) is a very malicious banking trojan, which is used in attempts to steal a wide range of victims' credentials.
- It was created for gathering personal information and stealing it without leaving traces.
- After hitting Japan in June 2014, it has since begun to surge in other geographies.
- This banking trojan can easily take over passwords, digital certificates, browser history and cookies.
- The final Vawtrak module also contains proactive protection against antivirus detection. This defense mechanism tries to detect any installed AV and disable it by using the Windows mechanism called Software Restriction Policies.

Geodo

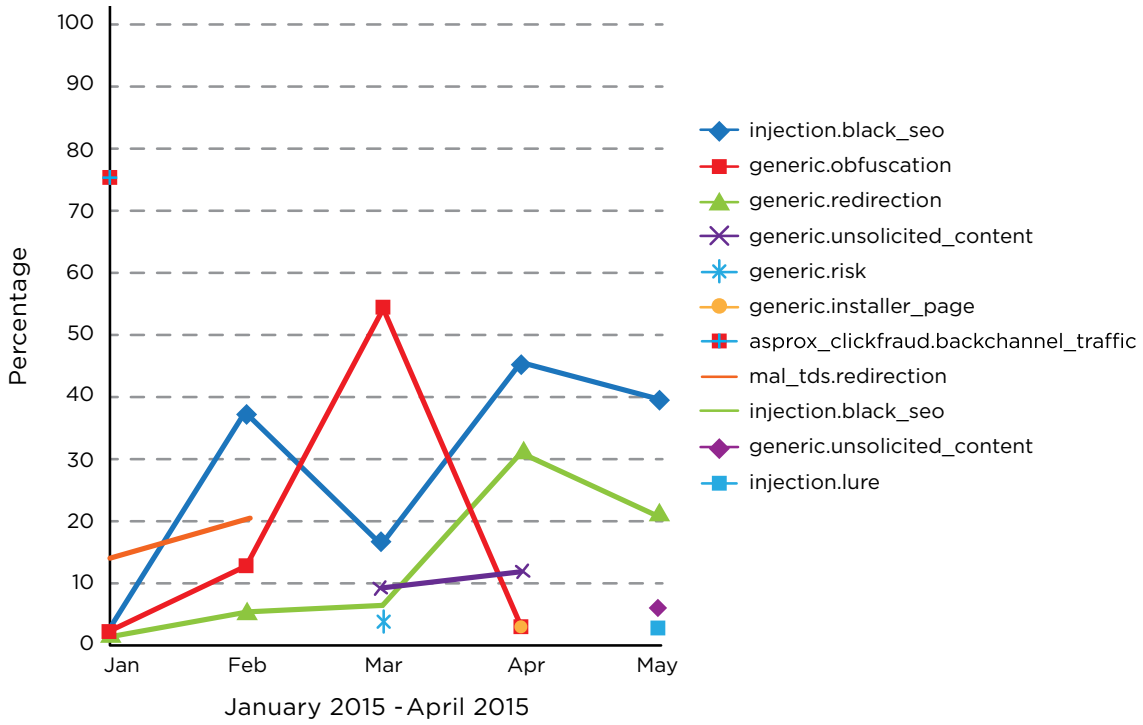
- While Geodo emerged to broad distribution in the summer of last year, the fact that it is seen in financial services more than 400 percent larger number of incidents is an anomaly specific to this sector.
- Geodo is an update of the Cridex attack, and has a separate email worm that looks to steal credentials and self-perpetuate in an industry, thereby initiating more lures.
- Geodo is a data stealing trojan that swipes everything from system information, credentials and much more.
- Geodo has been activated to attack bank security information through embedding automated scripts with repeating tasks into the macros of the Microsoft Office Package, continuing a pattern of increased use of macros in documents in attacks. Websense Labs noted this in its recent 2015 Threat Report. (vii)
- Geodo has a self-replicating feature that accesses a database of legitimate SMTP credentials from the Cridex botnet, sending small batches of infected emails from compromised hosts, while also presumably adding the newly compromised credentials to the pool of legitimate SMTP credentials.

Copyright © 2015 Raytheon Company.

4 FRAUDSTERS SWITCH-UP CAMPAIGNS FREQUENTLY TO OUTFOX BANKING SECURITY MEASURES

- Obfuscation and black search engine optimization continue to be more prevalent in attacks against financial services than other industries as a whole.
- Patterns in attack campaigns shift on a month-to-month basis, including huge spikes in malicious redirection and obfuscation detected in a wave of attacks in March 2015.
- This highlights an attack methodology designed for campaigns to be harder to detect and analyze by those charged with securing the finance sector.
- In addition, cybercriminals maintain a constant barrage of low-level attacks to keep security pros occupied dealing with a tremendous volume of background noise while targeted attacks are simultaneously occurring.
- Unsolicited content accounts for 10 percent of the security hits seen in financial services.

THREAT TYPES, FINANCIAL SERVICES – FROM JAN 2015 TO MAY 2015



- Similar to fluctuations in campaign techniques, countries hosting attacks against financial services vary from month-to-month, with a relatively high correlation to the specific techniques of campaigns.
- While the majority of the compromised hosts attacking the sector are consistently in the US, the geographic origin of specific campaigns fluctuates.
  - Fifteen different countries have rotated through the top five attack geographies in the last five months alone.

Copyright © 2015 Raytheon Company.

COUNTRIES IN WHICH THE THREATS TO GLOBAL FINANCIAL INSTITUTIONS ORIGINATE

Jan-15	%
U.S.	73.63
Russia	4.86
Germany	4.82
Poland	4.71
France	4.65

Feb-15	%
U.S.	35.15
Hungary	15.66
Serbia	11.82
Russia	8.69
France	8.38

Mar-15	%
Netherlands	46.93
U.S.	25.08
Germany	10.64
Latvia	7.27
Poland	7.02

Apr-15	%
U.S.	67.2
Bosnia & Herzegovena	17.91
France	6.05
UK	2.79
Canada	2.33

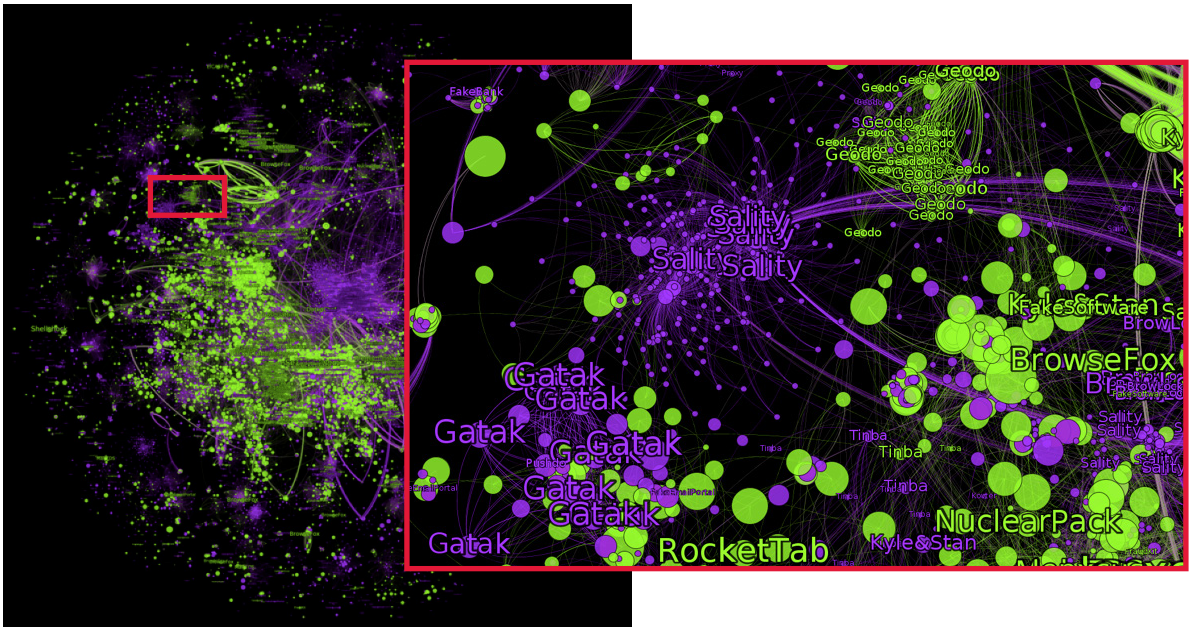
May-15	%
U.S.	61.1
Ukraine	10.4
Czech Rep	10.3
Serbia	6.9
France	2.8

Copyright © 2015 Raytheon Company.

CLUSTERING – FINANCIAL SERVICES

(SAMPLE RECENT WEEK OF DATA)

With attacks becoming more advanced and sophisticated each day, combining big data engineering, unsupervised machine learning, global threat intelligence and cybersecurity know-how is required to deal with them in a timely, automated and efficient manner. At a high level of abstraction, Threat Galaxy discovery is enabled by clustering across a broad, versatile definition of indicators that generalizes this approach across threat channels (such as email, web, file, reputation, etc.) while being able to dynamically model behaviors over time to observe changes and trends.



- The green nodes are threats impacting finance customers; purple nodes do not have an impact.
- The graph data was extracted by taking the threats impacting our customers and then crawling out to gather context.
- This shows how the finance sector sees a high volume of Geodo and low in Gatak.

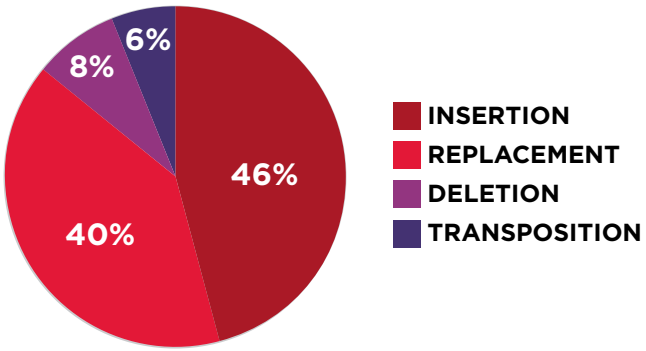
Gatak is a trojan with both data-stealing and back door capabilities. First discovered in 2012, it has included a number of revisions since that time, designed to more successfully evade detection by today's security measures. Affecting Windows computers, once the endpoint is compromised, the malware creates a number of registry changes to boot each time the computer is turned on. The malware collects system information and sends to a remote server by injecting code into the following processes: explorer.exe; winlogon.exe; and svchost.exe

Copyright © 2015 Raytheon Company.

5 FINANCIAL SERVICES RANKS THIRD FOR TARGETED TYPOSQUATTING

- While it may seem an antiquated methodology, the application of typosquatting has evolved into successful fraudulent incidents generating millions of dollars in financial losses and operational overhead.
- Websense researchers have seen an increase in the use of typosquatted domains in targeted attacks against financial services, usually combined with strong social engineering tactics.
- **When comparing more than 20 industries, financial services ranked as one of the highest for this highly successful type of attack.**
- These attacks are often combined with social engineering tactics via email to compromise hosts or to manipulate users (particularly in finance groups) to instigate an action (such as initiating an invoice payment or wire transfer).
- The average cost of such a spear-phishing incident averages to $130,000 per incident.
- There are many ways criminals use typosquatted domains in an attack;
  - *One of the most effective targeted attacks involves the use of .co domains, substituted for .com domains, particularly when combined with high-pressure social engineering.*

MOST POPULAR TYPES OF TARGETED TYPOSQUATTING SUBSTITUTIONS INCLUDE THE FOLLOWING:



- **TLD: .co**
  - While in our initial research, .co TLD was a hypothetical target for .com, we have found that Fraud Actors also used .co to target email domains, which end in .co.*, .com.*
- **Double-Character Insertion**
  - From the recently observed successful typosquat-driven campaigns, the Double-Character Insertion technique has been used more frequently than others
  - Popular characters include ll, ss, ii, tt
  - Placement: middle of the word
  - Benefit: The word is not visually widened/ lengthened
- **Single-Character Insertion**
  - Popular characters: i, l, r, t, s
  - Placement: middle of the word, beginning of the word
  - Benefit: The word is not visually widened / lengthened
- **Character Replacement**
  - Popular characters: i → l, e → a, g → q, o → 0
  - Placement: middle of the word, beginning of the word
  - Benefit: The word is not visually widened / lengthened
- **Character Replacement: TLD**
  - Popular characters: .co, .net
  - Placement: end of the word
  - Benefit: The change is not visually noticeable / identifiable
- **Character Transposition**
  - Popular characters: character order swap
  - Placement: middle of the word
  - Benefit: The word is not visually widened / lengthened
- **Character Deletion**
  - Benefit: Simple to execute and not always noticeable.

Copyright © 2015 Raytheon Company.

6 EVIDENCE INCREASINGLY SUGGESTS THE NEED FOR GLOBAL ECONOMY CONTINUITY AND CYBER INSURANCE MAY BE HINDERING REAL SECURITY ADOPTION IN FINANCIAL SERVICES

» The requirement for businesses in financial services to maintain their real-time connection to the global economy has impaired certain logical security precautions. *For example, a Wall Street Journal article (viii) noted:*

- A recent study suggested that while 90 percent of banks encrypt transmitted data, only 38 encrypt data at rest.
- Thirty percent of banks surveyed did not require multifactor authentication for third-party vendors.
- One Fortune 500 bank, for example, knows that several of its servers have not been patched for a serious bug called Heartbleed. The reason for the lack of remediation to eliminate this vulnerability, according to the bank's CSO who declined to be named for legal reasons, is patching these servers would break continuity with several European banks that have not yet upgraded their systems. This would disrupt their operations with its overseas partners.

» In addition, the emergence of cybersecurity insurance may only be providing a meager sense of false security. Banks with cyber insurance policies aren't necessarily fixing their security problems. Rather, they're relying upon their policies as financial liability risk management. But even that assumption is flawed. Cybersecurity insurance is limited in its coverage, and only partially limits the financial impact of a worst-case cyber-attack scenario.

- Eighty percent of banks have reportedly secured some cybersecurity insurance
  - » Comments from the CEO of U.S. insurer AIG suggest that the maximum amount insured by any one company (a bank) is $400 million. Most large corporate cyber insurance policies have a maximum value in the $100 million-$200 million range. (ix)
- A recent Standard & Poor's report noted that should successful and financially damaging attacks grow, the cost of insurance could rise or see restrictions regarding its availability. "In the worst case, the frequency and impact of attacks could mean that some companies or industries were deemed uninsurable, rendering them much more financially vulnerable." (ix)

Copyright © 2015 Raytheon Company.

CONCLUSION

For years, the finance industry has been under attack by highly specialized groups of criminals. The frequency and sophistication of targeted cyber-attacks is a top risk for this industry. By analyzing the actions and attack patterns prominent and anomalous to this sector we can share this knowledge to more effectively protect our customers' data and assets.

Threat intelligence, proactive prevention, faster incident detection and immediate response are critical for protecting against the risks presented by cyber threats. With valuable financial information and the sensitive personal information of millions of consumers on hand, businesses in finance must continually strengthen their security practices for effective defense and remediation efforts. Financial services organizations cannot rely on the insurance industry to protect them in the event of a catastrophic breach. Only with continued investment and increased understanding of the technology, tools and talent needed to effectively combat threats will the financial sector be able to mitigate the huge risk presented by cybersecurity threats.

i. "Ben Bernanke sounds warning on Cybersecurity", FinanceAsia, June 2, 2015: http://www.financeasia.com/News/398157,ben-bernanke-sounds-warning-on-cybersecurity.aspx

ii. "Travelers 2015 Business Risk Index Summary", May, 2015: https://www.travelers.com/prepare-prevent/risk-index/business/2015/business-risk-index-report.pdf

iii. ITRC Breach Reports, Identity Theft Resource Center: http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf

iv. "2015 ANNUAL REPORT", U.S. Department of the Treasury, May 19, 2015: http://www.treasury.gov/initiatives/fsoc/studies-reports/Documents/2015%20FSOC%20Annual%20Report.pdf; p. 4,9

v. "2015 Makovsky Wall Street Reputation Study", Makovsky Integrated Communications, May 28, 2015: http://www.makovsky.com/component/content/article/25-insights/articles/article/762-data-breaches-and-failure-to-protect-personal-info-further-damage-wall-streets-reputation-and-business

vi. "AS THE PRIVACY WORLD TURNS...SO MUST YOUR CYBER RISK MANAGEMENT LENS", Nadia Hoyte, Senior Vice President, Willis North America, April 2015: http://www.willis.com/documents/publications/Industries/Financial_Institutions/50928_PUBLICATION_Finex_Cyber_Alert.pdf

vii. "Websense® 2015 Threat Report", April 8, 2015: http://www.websense.com/content/websense-2015-threat-report.aspx

viii. "Financial Firms Grapple With Cyber Risk in the Supply Chain", Wall Street Journal, CIO Journal, May 25, 2015: http://blogs.wsj.com/cio/2015/05/25/financial-firms-grapple-with-cyber-risk-in-the-supply-chain/

ix. "Cyber Risk And Corporate Credit," June 9, 2015, Standard & Poor's Financial Services LLC

Copyright © 2015 Raytheon Company.