Malwarebytes

INDUSTRY SOLUTION BRIEF

Malwarebytes for Finance

Preventing and remediating financial cybercrime

THREATS FINANCIAL ORGANIZATIONS FACE

Ransomware

- Malware locks and holds financial data for ransom, interrupting productivity and putting trades and money transfers at risk.

Email phishing

- Hackers fake email communication among employees to trick them into opening attachments with malicious software.
- Customers bombarded with fake emails claiming to be from banks and financial institutions to collect personal information and credentials.

Threat proliferation

- Malware spreading across networked endpoints via infected email attachments or compromised files passed amongst employees.

Advanced persistent threats (APTs)

- Sophisticated attacker uses stealth and multiple attack methods to test and enter a financial organization.
- Attack is sustained over long time periods, probing the network.
- Difficult to detect, remove, and trace. (It took Yahoo two years to discover the theft of data on 500 million users in 2014.[9])
- Often involves back doors for ongoing access to gather intelligence.
- Malware can sit on financial institutions' endpoints an average of 98 days before being detected.[10]

Identity theft

- Stolen customer data containing date of birth, social security number, and other sensitive information used by cybercriminal to create false identities.

Social engineering

- Cybercriminals used publicized details of executives to trick employees into initiating wire transfers or opening spoofed emails with malicious attachment.

State of Finance

The financial services industry plays a vital role in the global economy for both commercial and retail customers. Its sectors span major banks and credit card issuers, insurance companies, pension funds, accounting firms, and stock brokerage companies, to stock exchanges, mortgage companies, and real-estate investment firms. They all represent a tempting target, inspiring a rising tide of cybercriminals who seek to steal money or information, disrupt operations, or compromise infrastructure. While cybersecurity is an obvious priority, it competes against business imperatives that can increase vulnerabilities to malicious activity. They include the need to become more agile and provide customers a seamless experience—whether the business transactions occur online, through mobile applications, or in the cloud.

Challenges Finance faces

Need for complete security visibility

Detecting threats and breaches across the security landscape calls for full awareness of all security events, whether it is before, during, or afterward. That includes threat and breach detection on endpoints, the ability to manage security events from a central location, and the capacity to collect system timelines and analyze breach details after they occur.

Complete malware remediation

Once a breach is discovered, it's imperative to remove the malware entirely. This can be a time-consuming and costly effort

if it requires re-imaging all the infected assets, or remediating the compromised endpoints deskside instead of resolving them remotely.

Regulatory compliance

In the face of the many cybercrime threats to finance and IT operations, federal financial regulators are setting expectations for the industry and holding it accountable for cybersecurity failings.

The Gramm-Leach Bliley Act, also known as the Financial Services Modernization Act of 1999, has a cyber-data component. It requires financial institutions to define safeguarding standards for protecting customer personal financial information from unauthorized access. It also authorizes fines of up to $100,000 for each violation.[1] Financial organizations face even more hurdles from different state regulators, who set out laws related to data breach notification, encryption requirements on portable devices, and the creation of comprehensive cybersecurity programs.[2]

Unauthorized network access

Financial service organizations are striving to grow, innovate, and optimize costs by adopting new business and technology practices. They want to connect with customers by new means, partner with third-party businesses across states and international borders, or outsource control of IT systems, all of which introduces heightened vulnerabilities across a multitude of access points.

For instance, skimmers and hidden cameras installed in ATMs capture credit card payment data, from which perpetrators create their own bankcards and steal from customer accounts.[3] Retail POS scams—such as the high-profile attack on Target—also capture payment data, and take weeks or even months to be discovered, much less mitigated.[4] Encouraged by banks, a significant percentage of customers already use 24/7 access to banking services on their smartphones and tablets, with projections that more than half the US adult population will bank by phone by 2019.[5] This represents a clear path for scammers as malware that steals consumer-banking information gets into mobile phones and waits for users to open a banking app.

According to a recent report, almost half of all data breaches at financial organizations take place through their websites.[6] Among the largest, most dramatic incidents is the one that took place in February 2016, when thieves siphoned off $81 million from a large, poorly secured bank in Bangladesh, using the SWIFT international messaging system to move the money. It happened when the fraudsters obtained legitimate SWIFT network credentials, made bogus transfers, and installed malware on bank computers to cloak their activities.[7] Moreover, a second attack on a SWIFT-connected bank has happened since then.[8]

External threats

Banks, credit card companies, and other financial organizations present an irresistible target for cybercriminals, from individual hackers seeking theft of sensitive information they can monetize to state-sponsored attackers with political agendas. Through malware, social engineering, or even by using employee insiders, bad actors are a fact of business life.

Data breaches are costly in ways that continue after a breach has been discovered and mitigated. Successful cyberattacks degrade a company's brand image, and therefore its bottom line. Reputation and brand perception are important assets, vulnerable to negative events. Consumer surveys indicate that data breaches are as damaging as poor customer services in how they affect brand reputation.[11] According to another study, once an attack has gone public, and financial organizations must advise consumers that their data is compromised, a majority of companies believe it can take 10 months to more than two years to restore a business's reputation.[12]

What financial organizations say

> Malwarebytes is a very effective tool. It's enabling us to enhance our overall endpoint security strategy with much better protection. It's easy to deploy and manage. Best of all, our users don't have to do anything, except continue to work without interruption.
>
> —Garfield Rodriquez, Group IT and Data Security, Sagicor Financial Corporation

> The threat environment is just going to get worse and the bad actors continuously get more clever. That's just the kind of risk we won't take. Malwarebytes makes sure we don't.
>
> —Russell Heelan, Network Administrator, United Bank

How Malwarebytes can help

Malwarebytes Endpoint Protection

Centrally protects financial organizations' endpoints against known and unknown attacks via cloudbased platform. Next-gen endpoint protection employs multiple layered protection technologies in a single unified agent to detect and block advanced threats, including ransomware.

Malwarebytes Incident Response

Rapid, lightweight solution detects and removes advanced threats from Windows and Mac endpoints. Scans and cleans infected endpoints remotely using an extensible cloud-based platform. Forensic Timeliner gathers system events surrounding breaches so the security team can address security gaps and reduce malware dwell-time.

[1]https://corpgov.law.harvard.edu/2014/09/10/cyber-security-and-cyber-governance-federal-regulation-and-oversight-today-and-tomorrow/
[2]http://ww2.cfo.com/cyber-security-technology/2016/02/financial-regulators-cyber-minds/
[3]https://archives.fbi.gov/archives/newyork/press-releases/2010/nyfo092310a.htm
[4]https://www.fbi.gov/news/testimony/cyber-security-enhancing-coordination-to-protect-the-financial-sector
[5]http://www.emarketer.com/Article/Millennials-Embrace-Mobile-Banking/1012871
[6]file:///C:/Documents%20and%20Settings/user/My%20Documents/Downloads/rp_DBIR_2016_Report_en_xg.pdf
[7]http://www.nytimes.com/2016/05/13/business/dealbook/SWIFT-global-bank-network-attack.html
[8]http://www.nytimes.com/2016/05/13/business/dealbook/SWIFT-global-bank-network-attack.html
[9]http://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html
[10]http://www.businesswire.com/news/home/20150519005417/en/Ponemon-Institute-Survey-Reveals-Time-Identify-Advanced
[11]http://www.darkreading.com/study-data-breaches-make-huge-impact-on-brand-reputation/d/d-id/1252742
[12]https://www.experian.com/innovation/thought-leadership/reputation-impact-data-breach.jsp

malwarebytes.com/finance corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes is the next-gen cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company's flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. More than 10,000 businesses worldwide use, trust, and recommend Malwarebytes. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia, and a global team of threat researchers and security experts.