E-NEWS

www.E-Safetech.om | 1-412-944-2402 |

March 2019

In this issue…

Cyberthreats and the finance sector

The financial sector has long been heavily targeted by cybercriminals. Over the years, the number of attacks that involved extortion, social engineering, and credential-stealing malware has surged rapidly. This means that financial institutions should strive to familiarize themselves with the threats and the agents behind them. Here are seven new threats and tactics, techniques, and procedures that security professionals should know about.

Extortion

Distributed denial of service (DDoS) attacks, which are typically delivered from massive botnets of zombie computers or internet of things (IoT) devices, have been used to bring down banking networks. This occurs when a targeted server or system is overwhelmed by multiple compromised networks. It's essentially like a traffic jam clogging up the highway, preventing regular traffic from arriving at its intended destination.

Some cybercriminals are relentless with DDoS attacks and follow them up with cyberextortion, demanding payment in return for release from costly downtime. Banks cannot defend against these attacks alone, so they rapidly share information among themselves through organizations such as FS-ISAC4 and rely upon the ability of their internet service provider to handle and redirect massive quantities of traffic.

Social media attacks

This happens when fraudsters use fake profiles to gather information for social engineering purposes. Thankfully, with new regulations such as the General Data Protection Regulation (GDPR), big companies like Facebook and Twitter have significantly enhanced their security and privacy policy with regards to their data handling practices. The unprecedented reach of social media is something companies cannot afford to ignore because of the possible implications a data breach can have on businesses.

Spear phishing
Spear phishing is an attack where cybercriminals send out targeted emails ostensibly from a known or trusted sender in order to trick the recipient into giving out confidential information. Over the years, hackers have upped their game and cast a bigger net, targeting unwitting employees to wire money. This attack is called business email compromise (BEC), where a fraudster will purport to be a CEO or CFO and request for large money transfers to bogus accounts.

Point-of-sale (PoS) malware
PoS malware targets PoS terminals to steal customer payment (especially credit card) data from retail checkout systems. Cybercriminals use a memory scraper that operates by instantly detecting unencrypted type 2 credit card data, which is then sent to the attacker's computer to be sold on underground sites.

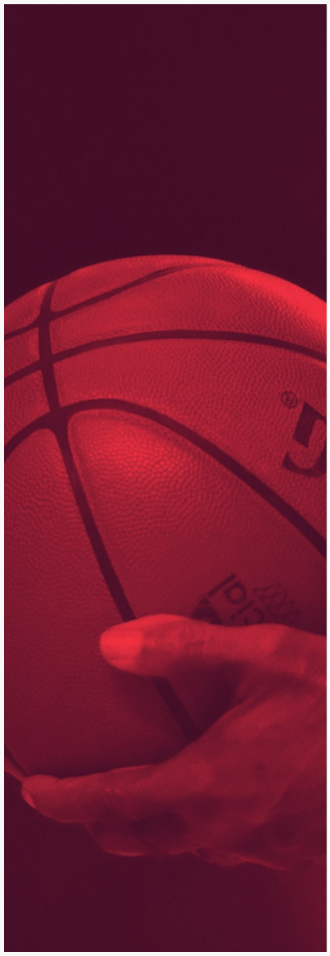
ATM malware
GreenDispenser is an ATM-specific malware that infects ATMs and allows criminals to extract large sums of money while avoiding detection. Recently, reverse ATM attacks have also emerged. Here, PoS terminals are compromised and money mules reverse transactions after money is withdrawn or sent to another bank account. In October 2015, issuers were mandated to shift to EMV or Chip-and-PIN system to address the weakness of the previous payment system.

Credential theft
Dridex, a well-known credential-stealing software, is a banking Trojan that is generally distributed through phishing emails. It infects computers, steal credentials, and obtain money from victims' bank accounts.

Other sophisticated threats
Various data breach methods can be combined to extract data on a bigger scale. Targeting multiple geographies and sectors at once, this method normally involves an organized crime syndicate or someone with a highly sophisticated set-up. For example, the group Carbanak primarily targeted financial institutions by infiltrating internal networks and installing software that would drain ATMs of cash.

Additionally, with the rise of cryptocurrency, cybercriminals are utilizing cryptojacking, a method that involves the secret use of devices to mine cryptocurrency.

The creation of defensive measures requires extensive knowledge of the lurking threats, and our team of experts is up to date on the latest security information. If you have any questions, feel free to contact us to find out more about TTPs and other weapons in the hacker's toolbox.



E-SAFE TECHNOLOGIES

E-SAFE TECHNOLOGIES PROUDLY PRESENTS THE 10TH ANNUAL MARCH MADNESS!

Tip Off: Thursday March 21st
9am
Where: McFadden's, 211 N Shore Dr, Pittsburgh, PA 15212
RSVP today!

TO SIGN UP VISIT

http://www.e-safetech.com/news-events/events/march-madness/

Lessons from a disaster recovery plan audit

Why do some companies fail their disaster recovery plan (DPR) audit? Perhaps because they did not get the right information for it. They say experience is the best teacher; thus, nothing beats what you can learn from real-world case studies. See what you can learn from the following case.

Hosting certain types of data and managing a government network legally bind you to maintain DRPs. After an audit of the Michigan Department of Technology and Budget, several failures led to a trove of helpful tips for small- and medium-sized businesses attempting to create a bulletproof disaster recovery plan.

Update and test your plan frequently
What was one of the first and most obvious failures of the department's DRP? It didn't include plans to restore **a**n essential piece of their infrastructure — the department's intranet. Without it, the employees are unable to complete even the most basic of tasks.

The reason for the oversight? The last time the plan was updated was in 2011, *leaving out more than six years of IT advancements*. If annual revisions sound like too much work, just consider all of the IT upgrades and improvements you've made in this year alone. If they're not accounted for in your plan, you're destined to fail.

Keep your DRP in an easy-to-find location
It may seem a bit ironic that the best way to store your top-of-the-line business continuity solution is in a binder, but the Michigan Department of Technology and Budget learned the hard way that the alternatives don't work. Auditors found the DRP stored on the same network it was meant to restore. Which means if something had happened to the network, the plan would be totally inaccessible.

Your company would do well to store electronic copies on more than one network in addition to physical copies around the office and off-site.

Always prepare for a doomsday scenario
The government office made suitable plans for restoring the local area network (LAN), but beyond that, there was no way for employees to get back to work within the 24-hour recovery time objective.

Your organization needs to be prepared for the possibility that there may not be a LAN to go back to. Cloud backups and software are the best way to keep everything up and running when your office is flooded or crushed beneath a pile of rubble.

Your DRP is more than just a pesky legal requirement. It's the insurance plan that will keep you in business when disaster strikes. Our professionals know the importance of combining both academic and real-world resources to make your plan airtight when either auditors or blizzards strike. Message us today about bringing that expertise to your business.

Will virtual containers change IT?

As technical as virtualization and virtual containers are, there's no reason your company shouldn't benefit from them. IT specialists all over the country are setting up and supporting these technologies for small businesses to increase efficiency and cut down on technology costs.

What are containers and why are they so popular?

Virtual containers are like digital versions of shipping containers, which use uniform packaging to simplify the portability and transportation of goods.

Virtual desktops, the predecessors to virtual containers, let users simply log into a web-based desktop, complete with a Recycle bin, Start bar, you name it. They're wonderfully convenient, but require a fair amount of computing power to run. The next logical step was to let users work from non-cloud desktops, but connect them to individual apps powered by servers across a local network or internet connection.

A qualified IT professional just needs to gather everything an app needs to run, put it in a container, and give users a way to access it. The servers that make this possible are designed to do all the work so users don't need high-end computers or specific oper-

What are the benefits of containers?

The best thing about virtual containers is its simplicity. Your IT technicians can make important applications available to the entire office without having to install them on each computer. This also means you don't need to worry about computers with limited hard drive space, incompatible operating systems, or slow processors.

Furthermore, when containers are updated on the server, the changes are immediately applied to any computer connected to the app.

The biggest obstacle to taking advantage of these benefits is the amount of technical expertise required to set them up and support them. It's not something most in-house technicians can keep up with if they're also in charge of day-to-day troubleshooting. Thankfully, the fact that containers can be accessed over the internet means IT providers can take care of most of the work remotely.

Want to maximize your business potential through virtualization and containers but need outside help? Call us today.

E-SAFE TECHNOLOGIES