the Availability Digest

www.availabilitydigest.com

FBI Warns Employees Are New Targets

November 2012

A recent joint report issued by several government agencies[1] concerned with cybersecurity has warned that individual employees at financial institutions are being more frequently targeted by cybercriminals. Prepared by the FBI (the U.S. Federal Bureau of Investigation), FS-ISAC[2] (the Financial Services – Information Sharing and Access Center), and IC3 (the Internet Crime Complaint Center), the report notes that cybercriminals are using a variety of malware to obtain employees' login credentials. The stolen credentials were used, for instance, to initiate unauthorized wire transfers ranging up to USD one-million dollars.

The increased attacks on "soft" targets are not limited to financial institutions. They are being launched against a variety of organizations that are not generally viewed as being obvious targets. The 2011 Data Breach Investigations Report (DBIR),[3] published by Verizon and the United States Secret Service,[4] suggests two reasons for this change in attack demographics:

- The success of law enforcement is the stick that is motivating cybercriminals to look for softer, less risky targets.

- The emergence of off-the-shelf powerful malware is the carrot that is making the effort of attacking small targets more attractive.

FS-ISAC, as a service to its members, sponsors weekly seminars on a variety of threats to financial institutions. A recent webinar focused on the FBI report. Presented by Dana Tamir, Director of Product Marketing for Trusteer, a major provider of endpoint cybercrime prevention tools, the webinar provides substantial material for this article.[5]

Cyberattacks

There many methods used by cybercriminals to attack IT infrastructures:

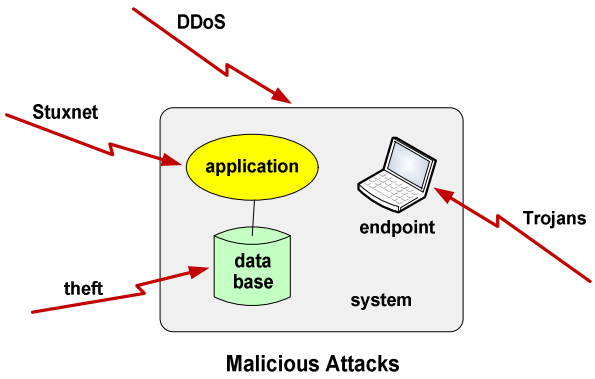
- *Distributed Denial of Service (DDoS)*, in which botnets are used to direct massive amount of traffic to a web site to overwhelm it. A recent very effective DDoS attack was directed at several

[1] Fraud Alert – Cyber Criminals Targeting Financial Institution Employee Credentials to Conduct Wire Transfer Fraud, *FBI, FS-ISAC, IC3 Joint Report*; September 17, 2012.
[2] FS-ISAC: Financial Services – Information Sharing & Analysis Center, *Availability Digest*; November 2012.
[3] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf
[4] Malware as a Service, *The Connection*; January/February 2012.
[5] Presentation: https://core.fsisac.com/FBI_WarnsEmployeesAreTheTarget.pdf
Recording: https://fsisac.webex.com/fsisac/lsr.php?AT=pb&SP=EC&rID=6037867&rKey=fc6e57b3afceceb0

large U.S. banks in September, 2012, by Islamic hacktivists in retaliation for the YouTube video, "Innocence of Muslims".[6]

- *Application compromise*, in which an application is corrupted to cause harm to an organization. Perhaps the biggest example of this is the June, 2010, Stuxnet virus which aimed to destroy Iran's centrifuges in its nuclear program.[7]

- *Data stealing*, in which massive amounts of confidential individual information is stolen from a hacked database. An example of this type of attack is the theft of the information of 100,000,000 Sony PlayStation accounts in April, 2011.[8]



Malicious Attacks

- *Endpoint attacks*, in which the devices that are the endpoints of the IT infrastructure, such as PCs and laptops, are infected to spy on the individuals using the devices. The sophisticated 2010 Flame virus was aimed at espionage of targeted systems.[9]

In its warning about employees becoming the targets of cybercriminals, the joint FBI/FS-ISAC/IC3 report focused on the increased activity to spy on individuals that are using system endpoints such as PCs and laptops.

Endpoint Attack Methodology

Cybercriminals are using advanced malware to infect the endpoint devices of organizations to steal the credentials of employees. They are infecting the endpoints with Remote Access Trojans (RATs) and variants of the Zeus malware. Remote Access Trojans (named after the classical Trojan horse) provide a backdoor for hackers to take control of the endpoint computer. Via the backdoor, the hacker can monitor the user's key strokes (key-stroke logging), can see his screens (screen capture), can include the device in a botnet, or can do virtually any other function that the user can perform.

Zeus is a Trojan horse like RAT that can be downloaded by botnets comprising millions of computers. There are an estimated 3.6 million Zeus-compromised computers in the U.S. alone.[10]

These Trojans typically use phishing emails and corrupted web sites to infect endpoint computers. If a user opens an infected file sent to him by email or accesses it on a phishing web site, the Trojan hiding in the email or web site will install itself on the user's computer, thus infecting it.

Once installed, the malware uses key logging and screen capture to monitor the user's activities and to steal his credentials and other confidential information such as bank account numbers and credit card numbers. Armed with this information, the cybercriminal can withdraw funds from the user's account, initiate wire transfers, and use the victim's credit card or debit card. In addition, if the hacker obtains login information to other systems used by the user, he can access those systems and extend his criminal activities.

Why are cybercriminals moving into these types of attacks? They are easier and safer. Corporations are putting a lot of effort into protecting their IT systems from cyberattacks. As the Verizon DBIR report

[6] Islamic Activists Attack U.S. Banks, *Availability Digest*; October 2012.
[7] Stuxnet – The World's First Cyberweapon, *Availability Digest*; March 2012.
[8] Sony PlayStation Taken Down For Weeks by Hackers, *Availability Digest*; May 2011.
[9] First Stuxnet – Now the Flame Virus, *Availability Digest*; June 2012.
[10] Zeus (Trojan horse), *Wikipedia.*

referenced earlier concluded, the success of law enforcement at tracking down major attacks coupled with the availability of off-the-shelf sophisticated malware is encouraging cybercriminals to look for softer targets.

Cybercriminals want to get around the security controls and get into a backdoor where they can focus on individual employees who are not the center of attention from a security viewpoint. There is less monitoring of employee activities than there is of major IT functions like database access. Endpoint attacks are becoming the preferred channel to perpetrate financial fraud.

Some Troubling Statistics

Mandiant (www.mandiant.com) is an incident response firm that does forensic analyses of attacks and works with their customers to create a remediation plan to mitigate its effects. They publish several reports on their findings. Among these are the following statistics:

- 54% of endpoint devices that were involved in an attack had been infected with malware and contributed to the attack. (The remaining attacks involved infections of the systems themselves.)

- 77% of the malware that is found on endpoint devices is commercial off-the-shelf malware easily available from public web sites for small fees (as the Verizon DBIR pointed out). Most endpoint attacks do not use sophisticated infections comprising malware that has been specially designed for the purpose.

- 94% of breaches are never discovered by the infected organization. They are reported to the organization by third parties, often days, weeks, or months later.

- 100% of breaches involving stolen credentials were made against endpoint devices that had up-to-date antivirus software.

The fact that organizations are unable to detect infections in their endpoint devices even with antivirus software is particularly troubling and makes endpoint attacks very effective. If days, weeks, or months elapse before companies are aware of an attack, it is too late.

Though antivirus software does an excellent job at preventing known threats, it is defenseless against zero-day attacks – those that occur before the virus has been identified. By the time that the virus is identified and included in the antivirus software, the endpoint device has already been infected and remains so.

Case Studies

Some examples of actual infections of endpoint devices are illustrative of the problems that organizations face with endpoint device infections.

- Hackers targeted a South African Postbank teller and stole his Postbank login credentials as well as those for several other systems. They then managed to transfer USD $6.7 million into their accounts. It is assumed that the teller fell victim to a scam email.

- An attack was launched against an international airline carrying thirty million passengers annually. A variant of the Zeus Trojan was used to steal the VPN credentials of an airline employee to log into the system. The attack used a combination of form grabbing and screen capture to obtain the credentials. To control the intrusion, the airline had to close down its VPN since this attack could compromise air travel security and border control.

- A Zeus variant targeted the Ceridian cloud-based payroll service. It stole employees' ids, passwords, company numbers, and the image-based secret authentication icons used to ensure employees that they had accessed the Ceridian web site and not an imposter web site. To protect against such attacks, Ceridian used a virtual keyboard that was accessed with mouse clicks so that there were no key strokes to intercept. But the malware used screen capture to detect the mouse clicks and to steal the information. The malware used in this attack was off-the-shelf malware not specifically designed to attack Ceridian.

- A RAT is commercially available online to target hotels. It steals the credit card numbers of guests as they check into the hotels. The RAT in question is called "Dark Comet." It can be found through Google, modified, wrapped, and used to target employees. Dark Comet can record key strokes, capture sessions, capture screens, and operate applications.

- Titon is aimed at attacking European and U.K. banks. It allows a hacker to modify web pages, to modify transaction content, or to insert additional transactions. It operates in a completely covert fashion evading antivirus detection. It is invisible to both the user and the host web application.

What these case studies show is that malware is very flexible and is continually evolving. It adjusts quickly to new security controls and learns how to evade them.

Attack Protection

There are several levels of security used today to prevent malicious infections.

Network Protection

Network Monitoring

Protection against malware begins at the network layer. The intent at this level is to prevent any malicious software from entering the system in the first place. Firewalls look for file names or signatures of known threats and block them. IPS (intrusion prevention systems) monitor traffic flows on the network and can stop an attack by terminating the network connection or user session originating the attack or by blocking access to the target from the user account or IP address. An IPS can reconfigure other security controls such as a firewall to block an attack.

Sandboxing

Another technique used at the network protection layer is "sandboxing." New executables received by a system or an endpoint are installed in an isolated virtual environment and monitored for a period of time. If they exhibit suspicious behavior, they are deleted. Since suspicious exectuables are never installed as operational software, they can do no damage. If they appear to be benign, they are allowed into the system.

Device Protection

At the device (system or endpoint) level, most devices run antivirus software. There are two types of antivirus software – black listing and white listing

Black Listing

Perhaps the most common prevention technique is black listing. Black listing is the technique used by antivirus programs that run on systems and endpoints. Known threats are identified by file names, signatures, or some other means. The antivirus software blocks any known virus from entering the system or endpoint. The number of new viruses increases dramatically on a daily basis, and the antivirus vendors identify these as quickly as they can and send updates to the protected systems and endpoints.

White Listing

White listing is the opposite of black listing. With this technique, signatures for all applications that are allowed to run on a system or on an endpoint device are maintained by the antivirus facility. An application can run only if its signature is on the approved list. If the execution of a malware process or of an infected process is attempted, its signature will not be on the list and it will not be allowed to run.

White listing provides a higher degree of protection than does black listing, but it imposes a heavy load on the security administration staff. New applications are continually added to the system. Existing applications are frequently updated. Applications may even modify themselves. As a consequence, legitimate applications are sometimes blocked from execution.

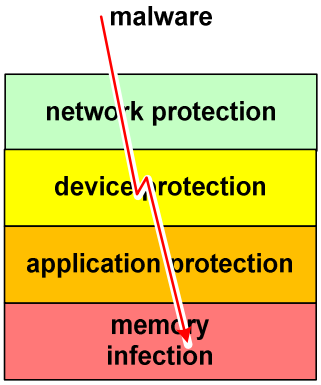
Evasion

Sophisticated malware is continually evolving and finding ways to evade these protections. Firewalls and antivirus facilities are bypassed by changing file names or signatures of malicious software. To defeat sandboxing, some malware will remain inactive for a period of time (minutes to days) until it is moved to an active environment, or it will wait until it detects some user activity such as mouse clicks that indicate it is in an active environment. White listing is evaded by using stolen vendor certificates to make the malware appear legitimate.

Another technique that is sometimes used by cybercriminals is to launch a DDoS attack on a site following a successful attack such as a large money transfer. This is intended to divert the attention of the organization's security staff so as to delay the detection of the attack.

Infection

Once a malware infection has evaded all of the security controls, it can install itself in memory. At this point, it is generally active and undetectable. There is no need for further evasion techniques. Until it is detected and blocked in an endpoint device, it can attack the VPN to get employee credentials by key logging or by grabbing screen shots of forms being filled out. Indeed, as experience has shown, the detection of an infection is often only by a third party and occurs days, weeks, or months later.



We will later discuss steps that can be taken to facilitate the detection and blocking of malicious infections that have taken hold of an endpoint device.

Anatomy of an Attack

Thus, there are four phases to a successful attack:

- *Lure* the user to download malicious software by getting him to go to a malicious web site and download something from that site or to open an email attachment that contains some malicious code.
- *Evade* all of the security controls.
- *Exploit* a vulnerability in an application or in the system or endpoint device.
- *Attack* the application or steal data.

It is sobering to note that 77% of the malicious code that is found in systems today is software that you can buy off the shelf.

Zero-Day Attacks

What is needed is better attack protection that can detect and delete advanced malware that has bypassed security controls before it enables a breach. This is especially important for zero-day attacks. A zero-day attack is an attack by malware that has not been seen before. Therefore, there is no antivirus protection for detecting and blocking it. It has no reputation attached to it upon which the antivirus can operate. It the malware gets by the firewall and other network protection facilities, it will infect the system or endpoint.

There are at least two facilities that can be employed to combat existing infections.

SIEM (Security Information and Event Management)

SIEM systems gather security-related events from a multitude of systems in the enterprise and organize them into a common database. There, sophisticated mining tools can be used to find suspicious patterns of operation.

If a system or endpoint has been infected, the infection may not be detectable but its activities will be. A SIEM can identify suspicious activity and quickly notify the organization's security staff so that it can investigate and take appropriate containment actions. Though this detection is after the fact, it will be much faster (minutes or hours) than the third-party reporting common today, which can take weeks or more. Thus, the damage caused by the infection can be significantly minimized.

An example of a SIEM tool is HP's ArcSight. ArcSight combines event data from all systems within an enterprise data center and analyzes it for data breaches. Malicious activity will often compromise several systems in order to achieve its goals, so being able to look across the enterprise is important.

HP's powerful fault-tolerant NonStop servers are interfaced to ArcSight via HP's XYGATE Merged Audit product from XYPRO Technology Corporation (www.xypro.com). Andrew Price, XYPRO's Director of Product Management, notes that "SIEMs are becoming an increasingly important weapon in the CSO's arsenal, because of the massive amount of audit data being generated across multiple disparate computer systems in a typical enterprise. This data needs to be normalised and correlated to be useful, and needs to be analysed as near to real-time as possible to ensure that any breach is quickly detected. In numerous breach scenarios, organisations have had audit data showing the breach occurred, but had not analysed the data and realised that there was an issue, resulting in days, and sometimes weeks, for hackers to continue their work undetected. XYGATE Merged Audit allows all audit and security event data from the HP NonStop to be included with the rest of the enterprise's audit data, ensuring a complete view of the entire organisation."

Trusteer Rapport

Rapport from Trusteer (www.trusteer.com) is a unique facility that it can rapidly detect malware directly in an endpoint device's memory. Thus, malware that has successfully evaded all of the other security controls in a system can be disabled by Rapport before it can take any actions. This ultimate layer protects an endpoint device wherever it is, even if it is being used at a user's home or in his travels where he is not protected by the corporation's network layer.

Rapport works by installing a small snippet onto the endpoint at login time. The snippet does not have to scan the machine or download any list of threats. It simply finds threats and disables any it finds. It accomplishes this via several mechanisms. It looks for suspicious actions, such as an application that is trying to install something or spin off child processes. If it finds such applications, it freezes them.

Trusteer notes that 77% of malware algorithms are known. It can therefore recognize these actions and block them. Rapport provides protection against well-known attacks such as key loggers, screen

catchers, process tampering, browser functions, and DNS poisoning. For instance, it will encrypt all keystrokes so that they are meaningless to malware. It ensures that API calls to capture screens are from a valid source. It prevents process modification.

It will validate sites to which the user is trying to connect and will reroute the user from a malicious site to the site he is actually trying to access. It will prevent users from using credentials on phishing sites.

Trusteer finds that 1% to 5% of the endpoint devices on which in installs Rapport have already been infected with undetected malware, which Rapport will then remove.

Actions that Rapport takes are reported to a central Trusteer repository for analysis by Trusteer specialists, and customers are notified of their findings.

Rapport is not a replacement for firewalls or antivirus software. Rather, it is the ultimate line of defense against malware that has managed to evade these security controls.

Summary

Cybercriminals are now directly targeting a company's employees rather than going after corporate systems. This is because law enforcement has become more successful at prosecuting cybercriminals who succeed in large attacks, and individual employee attacks garner less law-enforcement notice. Even so, the stealing of employee credentials can result in successful major attacks. This trend is aggravated by the off-the-shelf availability of powerful malware that can be used by cybercriminals to wage successful attacks with little effort.

The FBI in its report referenced earlier made several recommendations to improve security. Though there were several, they can be separated into four categories:

- *Educate* users about suspicious emails and malicious web sites.
- *Isolate* critical systems from the Internet so that there is no path for infections.
- *Process improvements* to add additional levels of review, approval, and auditing of critical activities such as wire transfers.
- *Tools* should be strengthened to detect infections and endpoint exploitations. The use of SIEMs and infection-detection tools such as Rapport are examples of tools that corporations should consider deploying.

No matter how smart we are at defending ourselves against malicious attacks, it seems that cybercriminals are always smarter. Whatever defenses we throw up are quickly thwarted by rapidly evolving malware. However, though endless, the fight must go on.