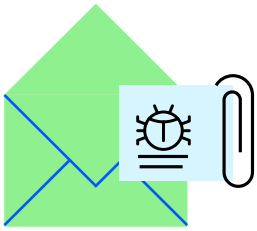
Progress® MOVEit®

Ransomware Vulnerabilities and File Transfer

WHITEPAPER



Introduction

It seems a day can't go by without a new cyber attack making the news. Fifty US banks were recently infected with the Trickbots Trojan. In 2016, cybercriminals stole $81,000,000 from the Bangladesh Bank by exploiting a pair of second hand routers. The recent Wannacry attack in Europe forced many hospitals to reroute their patients to other hospitals because they could not access their medical records.

In today's cyber security landscape it is important for IT and security teams to understand the attack vectors employed by cybercriminals and the vulnerabilities they exploit. One area that needs increased scrutiny is their file transfer infrastructure.

Changing attack vectors

The Symantec Internet Security Threat Report for 2016 highlights several key trends in cyber security. While data theft will always be a concern, they report that ransomware is on the rise.

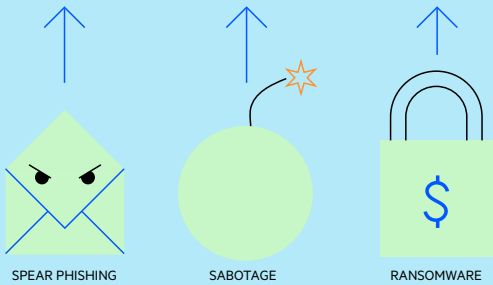
NotPetya is a high profile sabotage attack that victimized both Federal Express and Nuance. Each announced decreased earnings as a result of the disruption of services they offer their customers.

The Office of the Comptroller of the Currency (OCC) 2016 Semiannual Risk Perspective validates Symantec's findings. Addressing cyber security risks, they note that "phishing continues to be a primary method to breach data systems... the primary entry mechanism to perpetrate other malicious activity."

They warn banks that "Extortion campaigns have resulted in increased quantity and sophistication" and that "Successful attacks can disrupt a bank's operations and ability to provide services." They advise that organizations "Banks using un-patched or unsupported software and hardware enables the loss of data or customer breaches. A sound systems development life cycle... is essential to protecting against vulnerabilities."

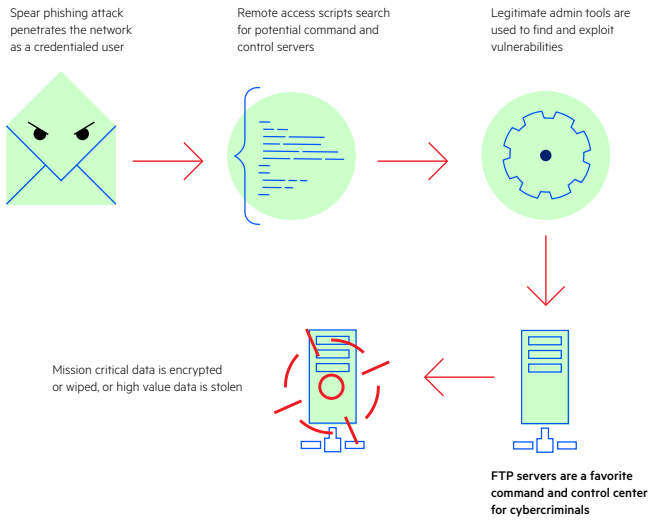
NEW ATTACK VECTORS

The Symantec *Internet Security Threat Report* for 2016 highlights several key trends in cyber security. While data theft will always be a concern, they report that ransomware is on the rise.



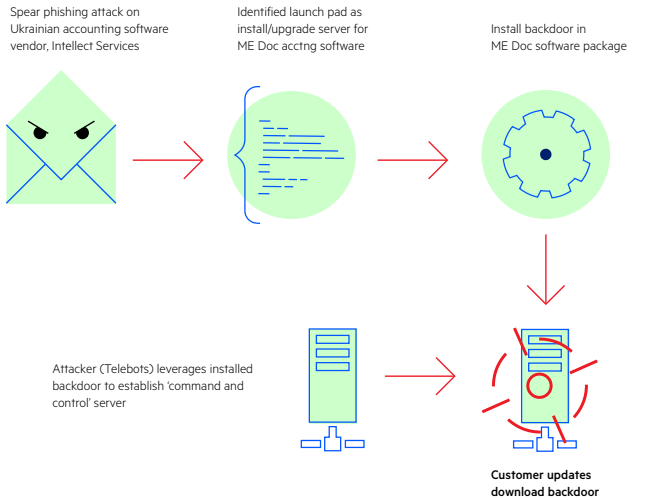
The anatomy of an attack

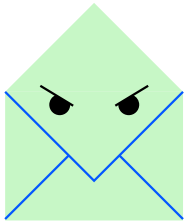
A typical attack has phases. First the attacker aims to clear the firewall, as well as any IDP/IPS, and access the network as a credentialed user. Then their objective is to find and gain control over a vulnerable device they can use as a command and control platform. Finally, they seek to deliver a malicious payload to critical assets on the network.



The NotPetya attack

One of the most devastating attack vectors in recent time is NotPetya. Originating out of Russia by the Telebots group, NotPetya first targeted Ukrainian businesses. It has since found its way to the U.S. NotPetya started off with a spear phishing attack on Intellect Services, the Ukraine vendor of M.E. Doc accounting software. Once inside, Telebots gained control over the M.E. Doc upgrade server. Vulnerabilities from old Open SSH, Web and FTP server releases made it an easy target. Telebots installed a back door in a .dll file in the M.E. Doc installation and upgrade package. Any customer who downloaded the package installed the back door. Telebots also installed command and control software on the M.E. Docs server to push NotPetya out to computers infected with the backdoor.





Spear phishing

Spear phishing is the practice of sending emails that appear to be from trusted individuals in order to convince an insider to reveal valuable information. The idea is to entice target users to open an email attachment or web link containing malicious software. For example, a script loading remote access software to gain control over the user's device.

It is the cybercriminal's penetration weapon of choice with several high-profile successes recently at the executive level of some of the world's largest banks.

The dark web provides hackers with access to spam tools, such as NECURS, which can pump out hundreds of thousands of emails per day. This increases the odds they can find an unwitting or untrained internal user who will fall into this trap.

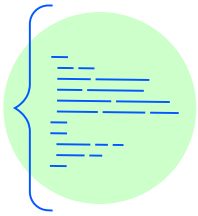
Spear phishing allows cybercriminals to clear firewalls and access the network as a credentialed user. It is a precursor to other malicious activities.

Searching for a "launch pad"

Once on the network, cybercriminals scan for insecure devices that can be used as a "launch pad" to attack high value targets. This can be accomplished through a number of tools that may or may not raise alarms in the security team.

After gaining control over the operating systems, they use legitimate admin and pen testing tools to traverse the network. After finding critical business systems, hackers deliver malicious payloads to steal data and/or disrupt business operations.

Password hashing offers little defense. You don't need a PhD in advanced mathematics to crack an encrypted password. You only need Google to download brute force programs like Cain and Abel or John the Ripper which can crack a Windows-based password hash in 2-3 hours. Multi-factor authentication is an effective counter measure when password hashes are cracked.



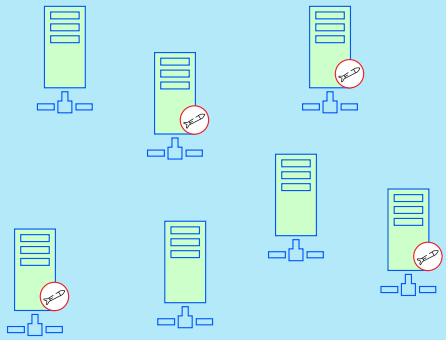
FTP servers as "command & control"

File Transfer servers, if not sufficiently secured, can be easy targets for experienced attackers. Those configured for anonymous access, where the login is often an email and the password may be "password", are the first and easiest target. An anonymous FTP server that is not properly segregated provides easy access to critical assets on the network.

The FTP protocol, without the added security of SSH or SSL, conveys data unencrypted. These servers are also often relatively unmanaged and there could be a large volume of information that is easily accessed and consumed that may be valuable or might aid the attack. Automation scripts and activity logs are often not protected. Hackers exploit this limitation to modify log files to cover their tracks.

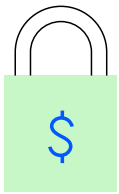
FTP SPRAWL INCREASES YOUR VULNERABILITY

IT often finds itself with dozens of FTP servers deployed across the network. We call this "FTP Sprawl". Many of these are clear text FTP servers and are one of the first targets cybercriminals look for.



IT often finds itself with dozens of FTP servers deployed across the network. We call this "FTP Sprawl". Many of these maybe configured in anonymous mode, send and store files in clear text FTP servers or depend on scripts. These are often the first targets cybercriminals look for.

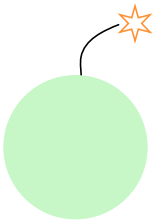
Earlier this year, the FBI issued an alert (FBI PIN 170322-001) that hackers were targeting clear text FTP servers configured with anonymous mode to launch attacks on the network. Many enterprise security, risk management, compliance and IT teams are now actively removing clear text and anonymous FTP servers from their environments.



Ransomware

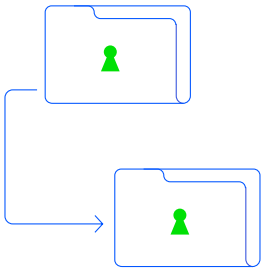
Once a command and control server has been established, the cybercriminal is able to target the assets that will achieve their objectives.

Ransomware attacks have received much visibility in the past year. The attack tactic is to identify valuable assets and render them unusable. By encrypting O/S or data files, or by changing passwords on critical business systems, cybercriminals can bring business operations to a standstill causing huge losses and potential regulatory exposures. Petya is an example of a ransomware attack in which files are encrypted and the user is prompted to make a payment in bitcoin in order to receive the key. Organizations anxious to get their businesses back up and running often pay up in one to two days.



Sabotage

Sabotage is also on the rise. The objective here is to actually damage the enterprise being attacked by destroying valuable data assets. Recent sabotage attacks employs disk wiping to erase all data and prevent its recovery. With no apparent monetary reward for such an attack, authorities now attribute sabotage to state sponsored or 'hactivist' groups.



Securing your file transfer environment

There are three critical steps that should be taken to secure your file transfer environment - consolidating, securing, managing.

Consolidating file transfer activity

FTP server sprawl is a fundamental security weakness. Typically the servers involved are on different operating systems, running different scripting languages and managed independently if at all. There is no uniformity in security or manageability. From a security standpoint, each represents an attack vector. Even if each system is well managed and has a complete audit trail of activity and access, auditors will look frowningly on the fact that there is no single audit trail.

Securing the file transfer environment

At a minimum, all servers should be upgraded to SFTP or FTPS. Either will encrypt data in transit and do not allow clear text passwords. Additionally using OpenPGP provides encryption to protect files at rest in the server directories. However, SFTP does not assure consolidation. Without consolidation, you still have multiple attack vectors and the risk successful penetration increases.

Managing the file transfer environment

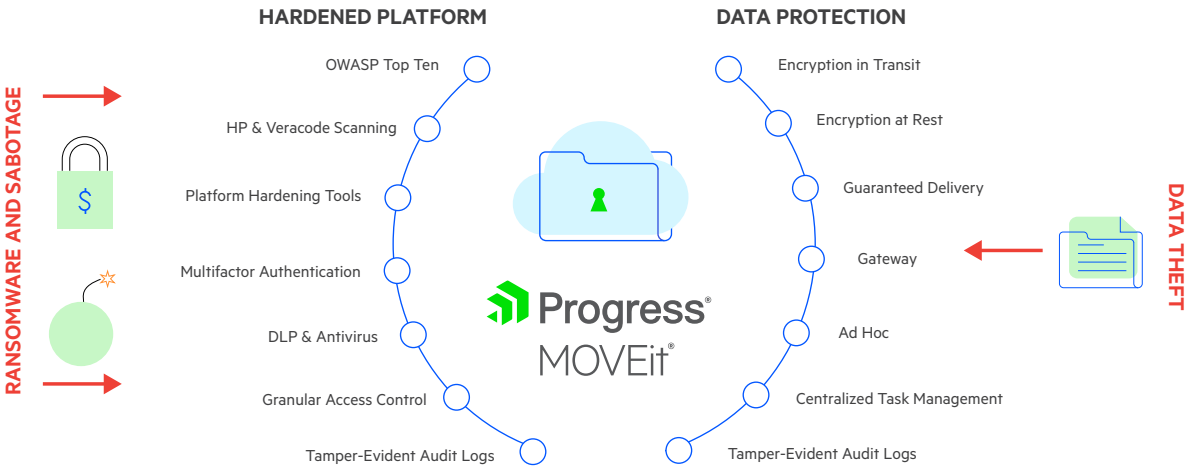
Centralizing management under one consolidated system greatly increases your ability to employ strong access and authentication controls, protect data both at rest and in transit, minimize the potential use of file transfer servers as command and control platforms and practice better file management hygiene.

MOVEit® secure managed file transfer

MOVEit provides a cost-effective alternative to clear-text FTP is consolidating your file transfer infrastructure. It protects against “launch pad” attack vectors with a hardened platform not found with clear text FTP or SFTP software. It is the only file transfer solution that is tested and validated against the OWASP Top Ten for the most critical application security risks.

Each release of MOVEit undergoes HP and Veracode dynamic and static scanning. These tools employ two different software testing methodologies to assess the security of an application. Dynamic testing uses penetration tests that inspect a running application and how it responds to various inputs. Static testing reviews and audits the application’s source code for vulnerabilities.

The MOVEit installation package includes platform hardening tools such as the SecAuxNET utility. It prepares the Windows Server platform running MOVEit for deployment on an Internet-exposed network segment. Some of the functions of SecAuxNet include:



To Learn more about how MOVEit can consolidate, secure and bring centralized management to your file transfer environment, please visit: www.ipswitch.com/moveit

For a free trial of MOVEit Transfer, please visit:
www.ipswitch.com/moveit-transfer-trial

About Progress

Dedicated to propelling business forward in a technology-driven world, Progress (Nasdaq: PRGS) helps businesses drive faster cycles of innovation, fuel momentum and accelerate their path to success. As the trusted provider of the best products to develop, deploy and manage high-impact applications, Progress enables customers to develop the applications and experiences they need, deploy where and how they want and manage it all safely and securely. Hundreds of thousands of enterprises, including 1,700 software companies and 3.5 million developers, depend on Progress to achieve their goals—with confidence. Learn more at www.progress.com, and follow us on LinkedIn, YouTube, Twitter, Facebook and Instagram.

Worldwide Headquarters

Progress, 14 Oak Park,
Bedford, MA 01730 USA
Tel: +1-800-477-6473

www.progress.com

facebook.com/progresssw
twitter.com/progresssw
youtube.com/progresssw
linkedin.com/company/progress-software
www.instagram.com/progress_sw_/

Progress