Preparing for Attacks that Seek Total Annihilation

The threat landscape has changed dramatically. Are you prepared for the new destructive attacks?

Written by Brian Hymer, strategic systems architect at Quest® Software, in collaboration with Randy Franklin Smith, Windows and Active Directory security expert

INTRODUCTION

IT and security pros have been battling serious threats for a long time. On the one hand are risks like power outages, hardware failures and natural disasters. On the other are malicious insiders and crafty hackers, armed to the teeth with innovative tools and techniques for exploiting vulnerabilities and creating increasingly sophisticated viruses, malware and ransomware.

Defending against these threats was never a picnic, but by and large, the risks were limited in important ways. Natural threats are generally contained in geographical scope, so having a backup datacenter in another location was an effective defense. And human attackers were usually focused on a specific goal: getting access to your data in order to either steal it and sell it for profit or to encrypt it and hold it hostage for ransom, so IT pros knew to prioritize data protection strategies.

But things have taken a decidedly ugly turn of late — more and more attacks are simply seeking the total annihilation of your infrastructure. Sadly, many organizations are simply unprepared. This white paper reviews some of the most destructive recent attacks, analyzes their speed, scope and methodology, and explores the best strategies for defending your organization against them.

THE SPEED AND POWER OF DESTRUCTIVE ATTACKS

You've undoubtedly heard the sci-fi-sounding names: NotPetya. Shamoon. Stuxnet. Olympic Destroyer. BlackEnergy. Destover. Wiper. Triton. But what actually happened in these destructive attacks? To get a sense of their speed and scale, and therefore the urgency of finding a strategy for defending against them, it's worth taking a moment to review a few recent incidents.

Stuxnet

In the late 2000s, Israel and the United States were increasingly concerned about Iran's nuclear program — by 2009, the country was producing so much enriched uranium that it was likely to be able to make two nuclear weapons within a year. In response, it is widely believed, Israel and the U.S. began developing a sophisticated computer worm, Stuxnet, designed not to hijack computers or steal data from them, but to destroy physical equipment. Specifically, when Stuxnet infects a computer that is connected to specific programmable logic controllers

(PLCs) that control industrial machinery like uranium centrifuges, it alters the PLCs' programming to force the centrifuges to spin too quickly and for too long, while ensuring that the PLCs continue to report that everything is working fine so anyone monitoring the equipment won't notice the aberrant behavior. Over time, the strain causes infected machines to tear themselves apart. In 2010, more than fifteen Iranian facilities were infected by Stuxnet, and almost one fifth of the country's nuclear centrifuges were ruined.

Stuxnet was never intended to spread beyond the Iranian nuclear facilities, which were air-gapped and not connected to the internet. Somehow, though, the malware did reach the internet and began to spread. Over time, other groups modified the virus to target other types of organizations, including water treatment plants, power plants, government agencies, and companies in the aviation, defense and pharmaceutical sectors. These modified viruses, sometimes called "the sons of Stuxnet," include Duqu, Flame, Havex, Industroyer and Triton.

> More and more attacks are simply seeking the total annihilation of your infrastructure. Too many organizations are simply unprepared.

Shamoon

In 2012, it was an oil company's turn to be hit by a destructive cyberattack. On Aug. 15, a virus later named Shamoon infected three quarters of the 40,000 workstations at Saudi Aramco, wiping their hard drives and displaying an image of a burning American flag. Although the company claimed that its oil production and exploration activities were not affected by the attack and that its main internal network was offline for just ten days, a consultant who was brought in to help with the recovery operation reported that Saudi Aramco had to rebuild its security operations center from scratch and that it was five months before its system were finally back online. He noted that the attack would have easily bankrupted a smaller corporation.

Shamoon disappeared from the headlines for four years, but in 2106, a slightly modified version of the malware was used against multiple government and civil organizations in Saudi Arabia and other Gulf states. The destructive malware reared its ugly head again in late 2018, hitting multiple targets in the Middle East. This new variant of Shamoon is even more destructive than the previous ones because it deletes all files from infected computers before wiping the master boot record, making recovery of the files not just difficult but impossible.

BlackEnergy

2015 marked the first successful cyberattack on an electric grid. In December, hackers using BlackEnergy malware were able to gain a foothold in several power distribution centers in Ukraine and knock electrical systems offline. Although this attack affected only about 225,000 customers and lasted just a few hours, it demonstrates the power of malware to bring down critical infrastructure. Future attacks on energy providers could prove far more devastating.

NotPetya

Perhaps the most far-reaching and expensive attack to date came in 2017. A finance executive at the Ukrainian office of international shipping giant Maersk had recently made a routine request: He asked IT to install an accounting software solution, M.E.Doc, on a single computer. Since M.E.Doc was not some random applications but the de facto tax accounting solution used by anyone doing business in the Ukraine, IT obliged. Then, on June 27, computers at Maersk's headquarters started going black. According to investigators, state-sponsored hackers had hijacked the update servers for M.E.Doc and used a back door to release malware into every company using the software.

Within hours, Maersk was effectively crippled. Every one of its 150 domain controllers worldwide, except for one in Ghana that luckily happened to be offline when the malware struck, was down. For days, its shipping terminals across the globe were frozen, with tens of thousands of trucks turned away and containers of perishable goods going without refrigeration. The cleanup involved rebuilding 4,000 servers and 45,000 workstations. A Maersk executive reported that NotPetya cost the company between $250 million and $300 million, although other insiders suspect the damage was higher.

But the damage was not limited to Maersk — NotPetya infected companies around the world, from Germany to the United States to Tasmania, at blinding speed. It took just 45 seconds for NotPetya to bring down the network of a large Ukrainian bank. A portion of one major Ukrainian transit hub was fully infected in 16 seconds. Practically every federal agency in Ukraine was brought to a standstill. The total damage was estimated at more than $10 billion.

Attacks in the cloud

Destructive attacks are by no means limited to on-premises IT environments, though not all of the incidents in the cloud to date involve malware with creative monikers. For instance, in 2014, IaaS provider Code Spaces went out of business after suffering a multi-stage attack on its servers; most of the company's data, backups, machine configurations and offsite backups were partially or completely deleted.

More recently, in February of 2019, hackers breached email provider VFEmail and formatted all the disks on every file and backup server in its U.S. infrastructure, destroying all the email data for its U.S. customers. The attackers also went after the company's IT resources in the Netherlands but were caught in the act, which enabled the company to salvage some of its backup data. Still, the attack erased virtually the company's entire infrastructure within just a few hours. The company expected to fold but it is still clinging to life.

THE MOTIVES BEHIND DESTRUCTIVE ATTACKS

Traditional attacks are typically motivated by financial reasons — for example, getting payment in exchange for the decryption key in a ransomware attack, obtaining PII or PHI that can be used for identity theft or sold on the black market, or harvesting user credentials that can be used in future attacks that yield financial gain. Destructive attacks generally have an entirely different set of motivations, including the following:

- **Political motives —** Hacking by nation states is increasing. For example, experts believe that Stuxnet was developed jointly by the U.S. and Israel to disrupt Iran's nuclear program, and that NotPetya was a politically motivated attack against Ukraine. Some believe the 2012 Shamoon attack was part of Iran's retaliation for U.S. involvement in Stuxnet. State-sponsored hackers are typically both highly skilled and well funded, so their attacks can be particularly devastating.
- **Social motives —** Some attacks are rooted in a desire for social change. Often dubbed "hacktivists," these groups often engineer denial of service (DoS) attacks against organizations they believe oppose their ideologies. For example, the hacktivist group Anonymous is perhaps best known for its 2010 DoS campaign that brought down PayPal.com and disrupted the sites of Visa and MasterCard in retaliation for those companies cutting off service to Wikileaks as required by the U.S. government.
- **Revenge —** At the opposite end of the spectrum is the disgruntled insider. For example, in early 2002, Roger Duronio, an IT admin at UBS Paine Webber, allegedly crafted a logic bomb and deployed it to thousands of systems using standard Unix admin tools. Then he quit and walked straight to his broker's office to place $21K in orders shorting UBS/PW stock. When the logic bomb went off a few weeks later, it brought down some 2,000 servers and deleted all the files on them. The damage was so severe that employees had to resort to pen and paper to conduct trades and other business. The company spent $3 million in consulting fees alone to get systems restored. Duronio's motivation? He was apparently disappointed with his bonus, which was $18K short of the $50K he was expecting.

  In a Windows environment, it's arguably even easier for a disgruntled privileged user to wreak havoc — all they have to do it take down Active Directory. If your AD is down, your entire network is down, even if there's nothing wrong with any of your servers or applications.
- **Smoke screen —** Increasingly often, hackers pair an attack designed to steal information with a destructive attack in order to cover their tracks. The destructive attack can hamper forensic investigations, making it difficult to identify the attackers, thereby preventing prosecution and protecting their modus operandi so they can continue using the same techniques in the future. For example, the Olympic Destroyer malware paralyzed IT systems ahead of the official opening ceremonies for the 2018 Winter Olympics in South Korea. But Olympic Destroyer covered its tracks so effectively that when it

> NotPetya brought down the network of a large Ukrainian bank in just 45 seconds. The total damage worldwide from the 2017 attack is estimated at more than $10 billion.

resurfaced later that year, targeting both financial organizations and biological and chemical threat prevention laboratories, researchers couldn't be sure whether it was being used by the same group or other groups with different interests.

- **Collateral damage —** Not all victims of destructive attacks are specifically targeted; some are merely collateral damage. For example, the architects of the NotPetya attack were clearly targeting Ukraine — estimates indicate that 80% of all infections were in that country — but companies around the world, including Maersk, suffered staggering damage.

METHODOLOGY

As we have seen, destructive attacks take a variety of shapes. Some involve malware or viruses, while others rely on brute force. Some try to erase data, while others seek to cause physical damage. Let's dig a little deeper into how they unfold.

> Any organization can be the target of a destructive attack — or simply collateral damage from an attack targeting somebody else.

Initial access

Usually, the first step in an attack is getting access to your network. You're probably familiar with many of the techniques, such as those listed below. It's important to emphasize that destructive attacks do not target just computers, such as workstations and servers; your attack surface also includes your IoT devices, routers and more.

- **Phishing —** Shamoon entered Saudi Aramco's network when an employee on the Information Technology team opened a malicious phishing email.
- **Backdoor —** A backdoor in the update software for a third-party business software solution enabled attackers to release NotPetya at Maersk and other organizations around the globe.
- **Infected USB device —** Since the Iranian nuclear facilities are not connected to the internet, Stuxnet had to be introduced through a physical USB device, either deliberately or accidentally.
- **Software vulnerabilities —** One technique used in the NotPetya attack, as well as in the WannaCry ransomware attack in 2017, was a penetration tool known as EternalBlue, created by the U.S. National Security Agency but leaked in a disastrous breach. EternalBlue takes advantage of a vulnerability in a particular Windows protocol, allowing hackers free rein to remotely run their own code on any unpatched machine.
- **Wi-fi or transmitter hijacking —** In 2015, the makers of the Jeep Cherokee were forced to recall 1.4 million vehicles after researchers demonstrated that they could remotely hijack the car's systems over the internet; attackers could potentially take control of a vehicle's door locks, brakes, engine or autonomous driving features. Similarly, the FDA confirmed that certain implantable cardiac devices have vulnerabilities that could allow a hacker to deplete the battery or administer incorrect pacing or shocks.
- **Vulnerabilities in IoT devices —** In October of 2016, the largest DDoS attack ever took down huge portions of the internet, including Twitter, Netflix, Reddit and CNN, by hitting a service provider called Dyn. The botnet used in the attack consisted of a large number of internet-connected devices, such as printers, digital cameras, baby monitors and consumer routers, that had been infected with malware called Mirai.
- **Vulnerabilities in other devices —** What would happen if someone reset all your routers, firewalls and wireless access points to their factory defaults or some other settings of their choice? Or hijacked them for their own purposes? In 2018, the FBI encouraged consumers to reboot their routers to help disrupt the spread of malware called VPNFilter, which researchers believe is being used by a group linked to Russian military intelligence to launch coordinated cyberattacks against Ukraine. The malware has since been upgraded so it can survive a reboot; everyone who uses any of the 70+ vulnerable devices is now advised to update the firmware immediately.[1]

Spreading inside the network and causing damage

Once malware has a foothold, it spreads from the infected machine to other computers on the network. One technique involves an exploit called Mimikatz, which enables hackers to harvest credentials left in a computer's memory and use them to access other machines. Sometimes, hackers hit the proverbial jackpot by scooping up

1 For more information, you can read the initial report from Cisco Talus about VPNFilter and the blog post in which it updates the list of affected devices. However, be sure to seek out the most up-to-date information using your favorite search engine or other research options.

powerful administrative credentials in addition to ordinary user credentials. In organizations that lack proper network segmentation and other security boundaries, malware can spread quickly, and more hands-on attackers can move laterally much more easily. Stealth tactics, combined with lack of continuous monitoring and alerting, often enables them to remain undetected.

Then the main part of the attack unfolds. Often, the goal is to wipe either specific data or the entire file system. To wipe the data, some attacks overwrite entire files, but since that takes time, other attacks take shortcuts that can be equally effective. For example, an attack might overwrite a 500-byte block every couple of megabytes, or simply overwrite the first N bytes of a file, which erases the header information. In either case, the technique renders the file useless even though it is not completely wiped. There's also destructive malware that goes against the boot subsystem (BIOS), as well as malware designed to disable services.

Often, an attack isn't triggered until the malware reaches saturation, to limit the victim's ability to spot the attack in time to take defensive action. To avoid a high I/O signature that could be more easily detected, malware often shifts the heavy lifting over to the bootloader. In addition, attacks are often timed to cause maximum damage; Both NotPetya and Shamoon were unleashed when many employees were off work to prepare for national or religious holidays, limiting the chances that the attack would be discovered promptly and limiting the ability of the victims to respond.

PREVENTION AND DETECTION STRATEGIES

Since any organization can be the target of a destructive attack or simply collateral damage from an attack targeting somebody else, every organization needs to take steps to mitigate their risk. The first step is to implement standard security best practices that help you prevent attackers from gaining access to your network, limit their reach and ability to move laterally if they do gain access, and spot their malicious activity. Here are some of the top strategies:

- Assign permissions based strictly on the principle of least privilege.
- Use a tiered security model to separate privileged users from regular business users, such as Microsoft's Enhanced Security Administrative Environment (ESAE), which is often called the "Red Forest" model.
- Don't allow untrusted code to run.
- Don't run outdated software and stay current on patches.
- Audit changes in your environment, and use tools that enable you to prevent changes to your most critical objects, such as highly privileged groups.
- Closely monitor configuration and other system changes and watch for unusual operations, such as commands that could alter boot partitions or brick a system.
- Monitor user activity, especially the activity of privileged accounts. Ideally, use a tool that creates a baseline of normal activity, looks for aberrations, and analyzes them in context to minimize alert fatigue while quickly spotting true threats.
- Automate response. Modern attacks unfold in seconds, so you can't afford to be content with a dashboard in your security operations center — by the time a human being spots an issue, investigates it and does something about it, the damage is done. Therefore, security automation and orchestration are essential.

DISASTER RECOVERY STRATEGIES

Layering together strong protection and detection strategies is crucial, but it's by no means sufficient. In many of the attacks described above, the victims were correctly criticized for various failures to implement security basics; for instance, at the time of the 2017 NotPetya attack, some of Maersk's servers were still running Windows 2000 — which Microsoft stopped supporting in 2010. Moreover, Maersk's insufficient network segmentation allowed the malware to spread easily from its initial foothold across the entire network.

But remember that Maersk did not do anything wrong to get infected in the first place. The malware was released via a standard tax accounting software package that nearly every company in Ukraine was using. Multiple organizations suffered crippling damage in the

> Strong protection and detection techniques are crucial but not sufficient; you also need a comprehensive disaster recovery strategy.

attack — and, like Maersk, most of them were not intended targets of the attack but merely collateral damage.

The lesson is clear: Even if your organization thinks it has no enemies and you implement all the security best practices experts recommend, you cannot guarantee that you won't fall victim to a destructive attack. Therefore, it's critical to have a tested and proven disaster recovery strategy in place.

Maersk didn't. They were saved only by a happy accident. When NotPetya took down all of its 150 domain controllers, no one could find a backup. If the company could not restore its DCs, it was dead in the water. But thanks to a local power outage, a lone domain controller in Ghana happened to be down at the time of the attack, and it proved to be the company's salvation. Unfortunately, the bandwidth at the Ghana office was so slow that uploading the data from the DC would have taken days, and no one there had a British visa, so the recovery team had to undertake a kind of relay race to bring the precious machine to the company's UK headquarters. But finally, they were able to use the machine to rebuild the other DCs.

If you suffer a catastrophic attack and have only native tools available, be prepared for a difficult, error-prone and lengthy forest restore process.

Reliance on a makeshift disaster recovery "strategy" like this is all too common, and far too risky. As we saw, the attack on VFEmail nearly destroyed the company; it's clinging to life only because some of its backup servers were saved. This case is particularly ironic, since the service which was set up in response to the ILoveYou virus that spread via email in 2001 and one of its key selling points was its ability to detect spam and malware. It's also particularly sad, since VFEmail had suffered multiple debilitating DDoS attacks over the years, but apparently failed to take them seriously enough.

Native tools

If you suffer a catastrophic attack and have only native tools available, be prepared for a difficult, error-prone and lengthy forest restore process.

Because AD forests are complex, with numerous interconnections between DCs, recovering an AD forest is challenging. Among other things, you need to:

- Reconstruct AD services
- Clean up metadata
- Re-establish trusts
- Reset accounts
- Restart replication

All of these tasks involve complex procedures that must be completed correctly; missing a step or performing certain ones out of order can cause the entire process to fail. Trying to complete a forest recovery manually with only native tools under the stress of a catastrophic failure with management breathing down your neck is an unenviable job.

To see for yourself just how tough it is, check out Microsoft's Active Directory Forest Recovery Guide, which provides a template for recovering an Active Directory forest if a forest-wide failure renders all DCs in the forest incapable of functioning normally.[2] Here is an overview of the high-level steps involved after you determine that a forest recovery is necessary:

1. **Determine how to recover the forest —** To prepare for the recovery, Microsoft recommends that you first determine the current forest structure, identify the functions that each DC performs, decide which DC to restore for each domain, and ensure that all writeable DCs are taken offline.

   Note that by Microsoft's own estimate, simply reading through this preparation step will take 12 minutes; the description of each sub-step is at least a page long.

2. **Perform the initial recovery (one DC in each domain) —** At a high level, the steps here are to restore the first writeable DC in each domain; reconnect each restored writeable DC to the network; and add the global catalog to a DC in the forest root domain.

   Completing just the first step — restoring the first DC — involves 13 separate sub-steps, some of which in turn involve multi-step procedures that are documented separately by Microsoft. For

2 Microsoft's Active Directory Forest Recovery Guide is available at https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-guide.

example, you need to create an isolated network, seize operations master roles, raise the value of the available RID pool, and remove the AD metadata of any DCs not restored from backup.

3. **Redeploy other DCs in the forest —** Once you have a stable forest with one DC for each domain and one global catalog in the forest, you can finally begin to redeploy other DCs in the forest by installing AD DS.

4. **Cleanup —** After the entire forest is recovered, you need to get users and line-of-business applications working again. Among other things, you need reconfigure name resolution (DNS), and determine what changes might have taken place between the time of the backup and the time of the disaster and then reapply them.

In addition to being complex and highly sensitive to human error, each of these steps can take a great deal of time. In fact, Microsoft acknowledges that "speed of recovery is not the primary goal" of its guide. The accompanying FAQ notes that most of the forest recovery steps can be accomplished using command-line tools and therefore you can write scripts to help automate parts of the forest recovery process. However, Microsoft cautions that you must thoroughly test your scripts before using them in an actual recovery, and that you need to update them whenever you make changes to your AD environment, such as adding a new domain or even a new DC, or upgrading to a new version of Active Directory.

Recovery Manager for AD – Disaster Recovery Edition

Fortunately, there are tools that automate the forest recovery process so you can get your organization back up and running faster and with far less effort and risk. Quest® Recovery Manager for Active Directory – Disaster Recovery Edition will help you implement a complete backup and recovery strategy to quickly recover from any disaster at the object and attribute level, the directory level, and the operating system level, across your entire AD forest. In fact, its automated recovery functionality can reduce recovery time from a DC-level AD disaster by up to 95 percent.

Quest On Demand Recovery extends AD backup and recovery at the object and attribute level to the cloud so you can protect not just on-premises environments but hybrid deployments as well. With On Demand Recovery, you can quickly and securely back up and recover Azure AD and Office 365, see both cloud-only objects and objects being synced through Azure AD Connect, run difference reports between production and real-time backups, and perform coordinated restores in both your on-premises AD and Azure AD.

CONCLUSION

Destructive attacks are on the rise, and their effects can be devastating. Every organization is vulnerable, whether as a direct target or simply collateral damage. After the devastating attack on VFEmail, its CEO and founder Rick Romero tweeted, "I never thought anyone would care about my labor of love so much that they'd want to completely and thoroughly destroy it." Don't make the same mistake.

To mitigate your risk, implement security best practices to block attacks, limit their reach, and help ensure prompt detection and response. But security experts and real-world attacks make it clear that you also need a comprehensive disaster recovery strategy. To learn more about how Recovery Manager for AD – Disaster Recovery Edition and On Demand Recovery can help, please visit quest.com/products/recovery-manager-for-active-directory-disaster-recovery-edition and quest.com/products/on-demand-recovery.

Implement a complete backup and recovery strategy across your hybrid environment with Quest Recovery Manager for AD and On Demand Recovery.

ABOUT QUEST

Quest provides software solutions for the rapidly changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid data centers, security threats and regulatory requirements. We're a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we've built a portfolio of solutions which now includes database management, data protection, identity and access management, Microsoft platform management and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (www.quest.com) for regional and international office information.