Combating destructive malware

Lessons from the front lines

IBM

Table of contents

Executive summary 1

What is destructive malware? 2

Timeline of destructive malware incidents 3

Who uses destructive malware, and why? 4

The impact and cost of destructive malware 5

Destructive malware activity is on the rise 6

What our team has learned about destructive attacks 7

How do threat actors get in and move around? 9

Sample attack flow for a destructive malware incident 10

How to better protect against destructive malware 12

Where is destructive malware going next? 16

Executive summary

Destructive malware that disables access to data or destroys system functions has been expanding across geographies and industries over the past few years. Organizations previously thought safe from this form of cyber aggression increasingly find themselves affected, either directly or indirectly.

The cost of a destructive malware infection can be significant for an organization. In fact, IBM X-Force Incident Response and Intelligence Services (IRIS) estimates that victimized organizations on average experience a total cost of over $200 million and have more than 12,000 devices destroyed in an attack. Recovery from destructive malware can also require hundreds of hours to remediate and rebuild environments that have been destroyed. The NotPetya malware that hit organizations across the globe is a stark example of the costly damage that destructive malware can leave in its wake. According to a White House assessment, NotPetya caused serious business disruption across geographies and resulted in more than $10 billion in total damages.

IBM X-Force IRIS' team of veteran intelligence and response specialists have amassed data and real-world experience from responding to and analyzing a variety of destructive malware incidents. In this report, the team draws on forensic investigations of destructive malware attacks to deliver valuable insight into these adversarial operations. Understanding the tactics, techniques, and procedures (TTPs) used by threat actors who leverage destructive malware can help organizations better assess risk, protect themselves, and prepare to respond to a destructive attack in accordance with their risk tolerance and business continuity goals.

This paper explores the changing definition of destructive malware, the impact it has on affected organizations, the lessons IBM has learned from our experience on the front lines, and what organizations can do to mitigate the risk. The final section in the report will also explore where we think this sort of adversarial activity might be going next.

What is destructive malware?

Destructive malware is malicious software with the capability to render affected systems inoperable and challenge reconstitution. Most destructive malware variants cause destruction through the deletion or wiping of files that are critical to the operating system's ability to run. They may overwrite the Master Boot Record (MBR), similar to the Shamoon malware, thereby corrupting the device's hard drive partition code and rendering it inoperable.

In a few cases—such as the Stuxnet worm—destructive malware used by nation-state actors was designed to destroy industrial equipment by sending tailored messages to turbines that caused them to malfunction and become inoperable.

Included in our definition of destructive malware is ransomware capable of wiping data from machines or irreversibly encrypting data on a machine. In some cases, this type of ransomware is *faux ransomware*, or ransomware claiming to desire financial gain, but does not allow decrypting the affected data even if the ransom is paid. NotPetya is a good example of faux ransomware. NotPetya prohibited decryption of data once machines had been infected, despite presenting victims with a ransom note demanding payment. Those who paid never saw their files decrypted in return.

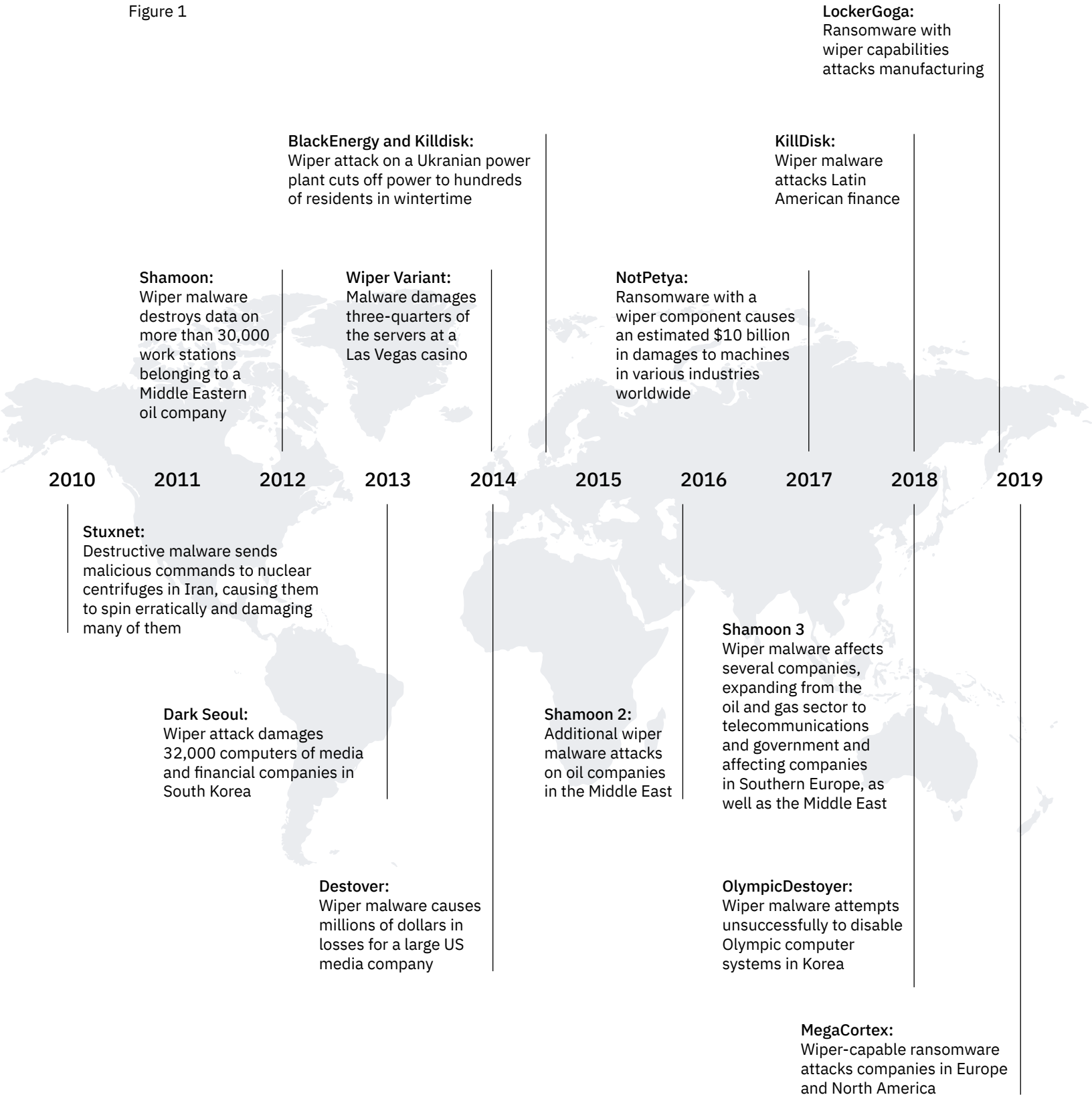
Historically, destructive malware such as Stuxnet, Shamoon, and Dark Seoul, was primarily used by nation-state actors. However, especially since late 2018, cybercriminals have been incorporating wiper elements into their attacks, such as with new strains of ransomware like LockerGoga and MegaCortex.

IBM X-Force IRIS views destructive malware as sophisticated malware with wiper capabilities, whether it's state-affiliated or criminal malware. The variety of industries targeted by destructive malware has expanded over time, especially through large, indiscriminate campaigns impacting multiple industry verticals.

[1]Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Timeline of destructive malware incidents

Figure 1



Who uses destructive malware, and why?

Between the years 2010 and 2018, destructive malware was primarily used by nation-state actors to further state interests. A classic intent of destructive malware is to cause harm to a geopolitical opponent. Some examples include the destruction of nuclear centrifuges in Iran, or debilitating operations of key industry organizations worldwide.

Further honing the capabilities of destructive malware, nation-state actors have been using attacks to project strength to their enemies. For example, Iranian attacks against their adversaries showcase their ability to cause harm with minimal repercussion. These efforts were launched predominantly by the Iranian hacking group known as APT33, tracked by X-Force IRIS as IBM Threat Group 02 (ITG02), which used Shamoon to target companies in the energy sector in the Middle East.

Destructive malware has also been used to deliver a political message while giving the attacking nation-state a level of plausible deniability, allowing them to claim ignorance to the activity while still affecting targeted entities. When used against a large US media company in 2014, for example, a destructive malware incident was designed to send a clear message of power and gave the perpetrator the ability to plausibly deny the incident. That malware attack was eventually attributed to North Korea.

Since 2018, however, X-Force IRIS has been observing cybercriminals increasingly incorporate destructive components, such as wiper malware, into their attacks on commercial entities. This is especially true for cybercriminals who use ransomware like LockerGoga and MegaCortex to infect enterprise networks.

Cybercriminals may be adopting these destructive elements to add pressure to their demands that victims pay the ransom—adding irreparable data destruction to encryption as a potential repercussion. Alternatively, criminals may be using wiper malware to lash out at victims if they feel wronged, using destructive attacks more impulsively rather than strategically.

The impact and cost of destructive malware

The amount of damage companies experience in a destructive malware attack can be difficult to quantify, but X-Force IRIS has assembled some informed estimations based on our analysis of several publicly disclosed attacks. On average, large multinational companies appear to incur costs around $239 million, per incident, according to our analysis of several publicly disclosed attacks. These estimates include the cost of remediation, equipment replacement, lost productivity, and other business damages. This number is 61 times greater than the cost of a typical data breach, which the Ponemon Institute places at $3.92 million on average for companies worldwide, underscoring the significant cost destructive malware attacks can incur. For most companies that experience a destructive malware attack, this cost will make a marked impact on business earnings for multiple quarters or even years after the incident.

In addition, the average number of workstations rendered unusable in a destructive malware attack is approximately 12,316, according to X-Force IRIS analysis of publicly disclosed attacks. The size of a company and number of devices and servers it houses will have a significant impact on the number of workstations a destructive attack affects. In many destructive malware attacks, the number of workstations affected may be as high as three-quarters or more of the total network. The level of destruction caused by the attack often requires a complete and rapid replacement of the equipment.

For incidents involving destructive malware to which X-Force IRIS has responded, the average number of hours needed to remediate the incident was 512, stretching to 1,200 hours or more for significant events. This number includes cases where the malware was not deployed, cases where equipment simply needs to be replaced with limited remediation options, and where X-Force IRIS is working in conjunction with other teams that add additional hours to the total. Compared to non-destructive attacks, this number of hours committed to remediation alone is rather high.

Figure 2: X-Force IRIS Estimates for the Cost of Destructive Malware (Source: IBM X-Force)

$239m

Average cost to a large multinational company experiencing a destructive malware incident

12,316

Average number of computer workstations and servers destroyed in a destructive malware attack

512

Average number of remediation hours X-Force IRIS incident responders spend remediating a destructive malware attack

Destructive malware activity is on the rise

X-Force IRIS data shows that destructive malware—including ransomware that leverages a destructive element such as wiping—is becoming more prevalent in attacks on companies worldwide. Overall, X-Force IRIS incident response teams have assisted victimized organizations with 200% more destructive malware cases in the first half of 2019, when compared to the second half of 2018. Of those destructive malware cases, 50% targeted organizations in the manufacturing industry. Other sectors significantly affected included oil & gas and education. Most of the destructive attacks we have observed hit organizations in Europe, the United States, and the Middle East.

In addition, ransomware attacks containing a destructive element have spiked in 2019, as new strains of ransomware such as Locker-Goga and MegaCortex entered the cybercrime arena. X-Force IRIS incident response data indicates that ransomware attack calls to our emergency response hotline have more than doubled over the past twelve months, with an increase of 116% from the second half of 2018 compared to the first half of 2019. While not all ransomware attacks incorporate destructive malware, the simultaneous increase in overall ransomware attacks and ransomware with destructive elements underscores the enhanced threat to corporations from ransomware capable of permanently wiping data.

We anticipate that cybercriminals' use of destructive ransomware will increase over the next five years, given a perceived success of cybercriminal groups currently using these tactics and the potential for proliferation via dark web marketplaces.

Figure 3: X-Force IRIS Data Demonstrates Destructive Malware Attacks are on the Rise (Source: IBM X-Force)

200%
increase

In X-Force IRIS incident response cases of destructive malware from July—Dec 2018 to Jan—July 2019

116%

increase of ransomware attacks observed by X-Force IRIS over the past twelve months

50%

of X-Force IRIS destructive malware cases affected the manufacturing industry

X-Force IRIS has observed destructive malware attacks in the

USA
Europe
Middle East

What our team has learned about destructive attacks

We are up against creative humans. Most groups we have observed conducting destructive malware attacks are sophisticated, stealthy, and take great care to cover their tracks. Yet it is apparent that the actors behind the activity are still human, and not robots. We have tracked changes in behavior by destructive malware attackers when they find incident responders are conducting detection and containment work on networks they have compromised. They lose composure, unwittingly reveal their actions, and react in ways that can prevent them from accomplishing their objectives.

We have also seen financially motivated attackers switch to destructive tactics when they perceive they are not achieving their objective with the targeted organization, using destruction as a means of revenge. The more an organization understands the human motives behind the activity and what the attacker may be after, the better they can foresee and handle a potential destructive malware attack.

Attackers are often present on a device, asset, or network for weeks or months before carrying out a destructive malware attack. We've observed attackers reside in targeted environments for over four months prior to launching a destructive payload, giving them ample time for internal reconnaissance where they map out the infrastructure and find ways to achieve their objectives. This in-depth reconnaissance from within the network and patience for the slow-and-steady strategy may allow threat actors to more effectively damage operations, but they also provide defenders with a significant opportunity to detect and neutralize the threat before it can take effect.

Attackers will often preserve any access to critical devices for the destructive phase of their attack. Maintaining access to critical systems allows attackers to maintain control of their strongholds for as long as possible, and to cause as much damage as they can. Access points and key infrastructure are of particular value to threat actors during this phase. Finding and neutralizing them can help mitigate an attack in progress.

Prevention is ideal, but isolation is critical. Though preventing a destructive attack is always ideal, it cannot always be prevented. But even in cases where an attack materializes, if the affected parts of the infrastructure are isolated, an organization can significantly limit the damage and prevent some of the impact to its operations.

Reducing the number of devices affected by a destructive attack can also drastically reduce the cost and time associated with reconstitution. Since we see threat actors leveraging third-party access to break into targeted networks, it is imperative to further implement isolation of critical systems from potential third-party infections.

"There are two forms of targeted attacks in the destructive world: 'I need to be low and slow until I gather the information I need and plan out my attack' [. . .] or, 'I'm going to drop in, release, and let it go wild.'"

– Christopher Scott
Global Remediation Lead, IBM X-Force IRIS

How do threat actors get in and move around?

Initial infection vectors

Initial infection vectors for destructive malware tend to involve spear-phishing emails, credential compromise through password guessing or brute-forcing, watering-hole attacks, and compromise of third parties.

Phishing emails

X-Force IRIS has observed that phishing emails used in destructive malware attack incidents varied significantly in the level of sophistication. The more sophisticated phishing emails often included documents with malicious macros that appeared legitimate, or in some cases were altered versions of legitimate documents and contained language that demonstrated a level of fluency in the target's language.

Credential compromise

Password stealing or guessing remains a popular infiltration tactic for threat actors, and this method of getting and using compromised network credentials has been successfully leveraged to gain a foothold in some of the largest destructive attacks.

In the case of Shamoon attacks, threat actors brute-forced a network user's password to gain initial access, and in LockerGoga attacks, actors used stolen employee credentials to do the same. In both cases, multifactor authentication was not implemented and could have offered an additional layer of protection when compromised credentials were then used by the attackers to get in.

Watering-Hole Attacks

Watering-hole attacks are another infection vector threat actors use to gain access to target networks in preparation for destructive malware attacks. The watering-hole technique targets and manipulates web pages frequently visited by members of the target organization or sector, turns them into a malware infection zone, and ultimately allows attackers to launch drive-by downloads of their malware on that page, or to steal information with no additional action required from the user.

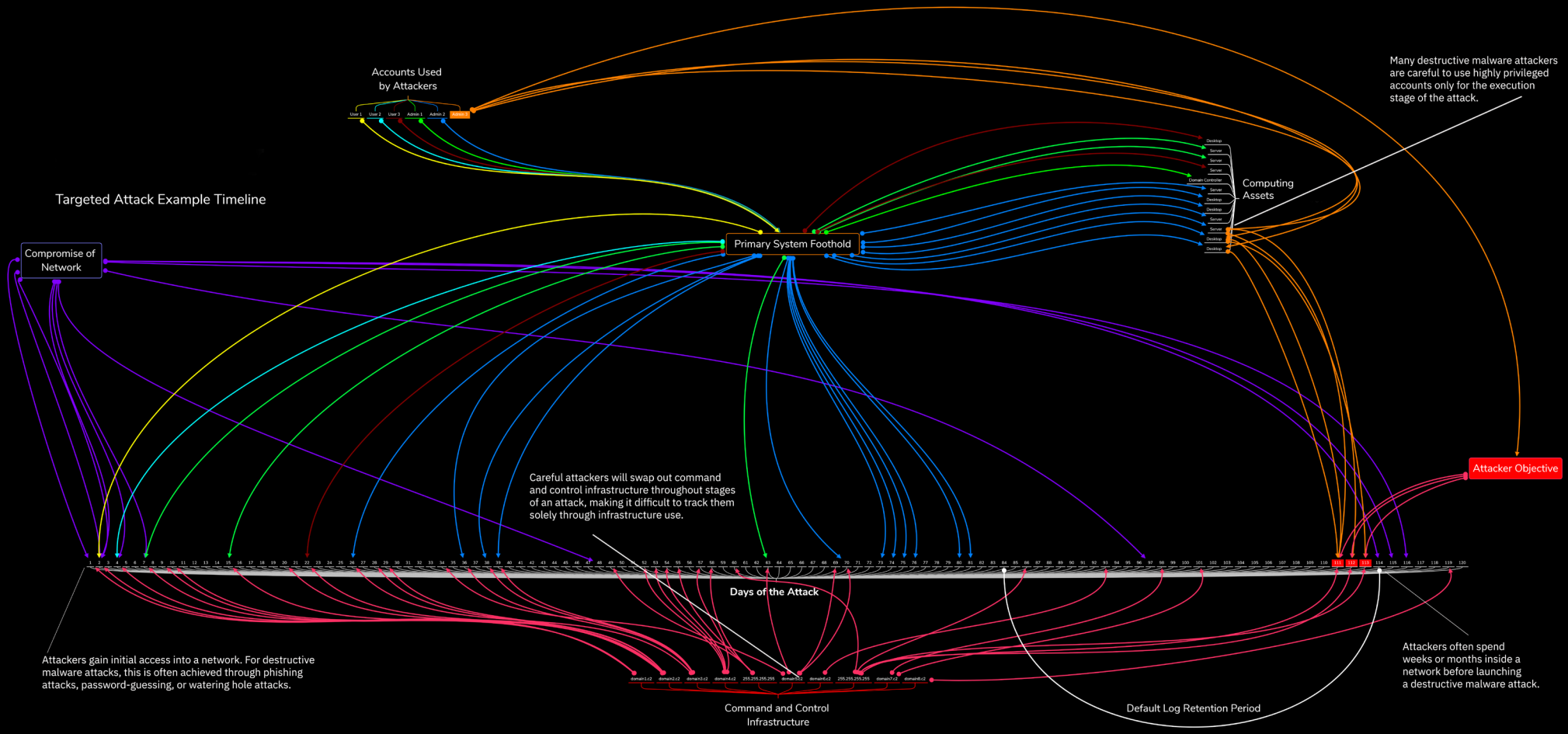
Compromise of Third Parties

Third-party compromises have likewise provided an avenue of access for attackers seeking to conduct destructive malware attacks on an organization. In the NotPetya attacks, a patch legitimately pushed to users of a tax accounting software in Ukraine served as the primary infection vector in an attack that spread quickly and widely to a large number of organizations across the world.

[2]Dennis Fisher, "NotPetya Hits the Soft Underbelly of the Patching Process," Digital Guardian, July 26, 2017, https://digitalguardian.com/blog/notpetya-hits-soft-underbelly-patching-process.

Sample attack flow for a destructive malware incident

Figure 4



Lateral Movement

Lateral movement in destructive malware attacks tends to follow one of two trends: privileged account takeover, or the use of PowerShell scripts. These vectors are the most commonly observed by X-Force IRIS responders in cyber incidents across a wide spectrum of attack types, including destructive malware cases.

Privileged Account Takeover

Threat actors are increasingly targeting privileged accounts and services for lateral movement. In many of the cases our team analyzed, threat actors used privileged accounts to move between network devices and assets. Unlike attempting remote access, which can generate significant noise, moving laterally with a privileged account can allow the adversary to stealthily move between devices while appearing to be legitimate administrative activity. In some attacks, X-Force IRIS responders saw attackers use a privileged account to wipe an organization's entire email system, which further challenged the organization's ability to respond to the incident.

PowerShell Scripts

PowerShell, a Microsoft framework that is both a scripting language and a command line executor, first appeared in 2006 and has been a standard feature of the Windows operating system ever since. PowerShell scripting has been increasingly gaining popularity among adversarial actors since 2016 as one of the most frequently used lateral movement techniques observed by X-Force IRIS incident responders, and destructive malware attackers have followed this trend.

Modern ransomware variants, such as MegaCortex, can use malicious PowerShell scripts to move between networked devices. In many cases, PowerShell is native to the operating environment, making it appear legitimate and thereby more difficult to identify as anomalous activity, which can further challenge detection and response.

How to better protect against destructive malware

Test your response plan under pressure. Use of a well-tailored tabletop exercise and a cyber range simulation can help ensure that your organization is ready on both the tactical and strategic levels for a destructive malware attack. Playbooks can sometimes crack under pressure, and that is when muscle memory becomes important—your team must know what to do automatically and respond decisively in the critical moment. Exercising incident response procedures also provides an opportunity to cultivate a culture of security within the organization and get leadership involved so that they understand the situation and can make the best decisions at the right time. Mature response plans require testing and adjustment, and with proper training, defenders can work to ensure that team members know the plan and will be able to implement it effectively when the time comes to respond and remediate.

Use threat intelligence to understand risks to your organization. Each threat actor has different motivations, capabilities, and intentions, and threat intelligence can help provide insights that increase the efficacy of an organization's preparedness and eventual response to an incident.

Also, by having a better understanding of the threat landscape through robust intelligence, organizations can better optimize security spending to protect against destructive threats. If an organization knows it may be targeted by a sophisticated actor intending to cripple operations, they can redirect security spend toward practicing quick reconstitution in the face of an overwhelming destructive attack that might have been underway for months before its discovery. Threat intelligence allows the organization to choose to practice the relevant response scenarios, versus selecting them at random.

Engage in effective defense-in-depth. Incorporate multiple layers of security controls across the entire Cyberattack Preparation and Execution Framework.

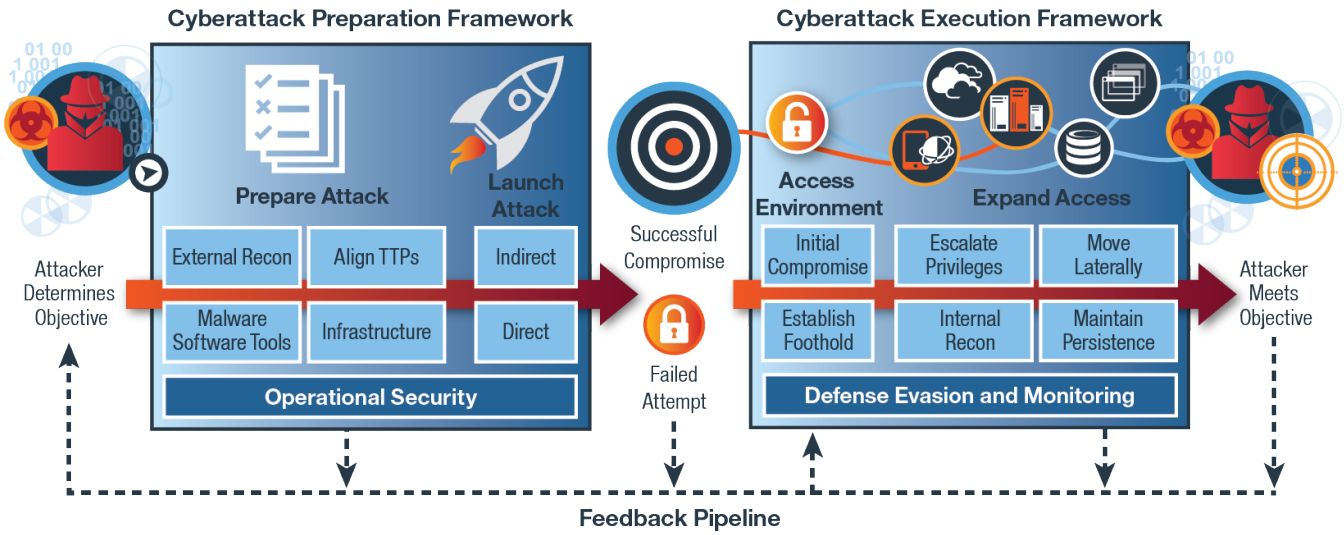


Figure 5: X-Force IRIS Cyberattack Preparation and Execution Framework (Source: IBM X-Force)

Having effective preventative, detective, and corrective controls in place is critical for reducing risk. In many cases investigated by X-Force IRIS, destructive malware evaded antivirus detection long enough to execute the payload, which means that organizations need to rely on additional, layered controls to find and stop this type of malware. An effective endpoint detection system can further enable detection of malicious activity within the organization's perimeter.

[3]"IBM X-Force IRIS Cyberattack Preparation and Execution Frameworks," IBM X-Force IRIS White Paper, July 2018, https://securityintelligence.com/media/ibm-x-force-iris-cyberattack-preparation-and-execution-frameworks/.

Reduce privileged accounts within the environment. Our team has frequently observed threat actors leveraging privileged accounts to move freely within a targeted environment. By segregating account privileges, reducing them to a minimum, logging admin account activity, and applying multifactor authentication to these accounts, organizations can restrict this convenient lateral movement technique.

Furthermore, organizations should ensure that the same account cannot be used to access every critical system. If such an account is needed, organizations should put protections in place to prevent compromise and have that account closely monitored. "When we think of today's environment, especially in the Active Directory world, we should not have a single user account that has access to everything," X-Force IRIS Global Remediation Lead Christopher Scott notes.

Implement Multifactor Authentication (MFA) throughout the environment. According to Christopher Scott, "multifactor authentication is a must in today's world." The cost-benefit ratio of MFA implementation is tough to overstate in cases where it can minimize the window of opportunistic attacks. As an added layer of security, MFA can provide significant security benefits in reducing the value and the potential of stolen or guessed passwords for attackers who do not intend on investing more heavily to take over a user's account. In short, MFA implementation can help reduce the entry vectors into an organization for threat actors and in many cases also prevent the successful use of compromised privileged accounts for lateral movement.

Baseline internal network activity and monitor for possible lateral movement. Destructive attacks become most harmful when they spread, and a common lateral movement technique is leveraging existing accounts the attackers manage to compromise.

To detect and remedy misuse of user accounts, organizations need to baseline standard day-to-day activity and alert on anomalous behavior, such as an administrator logging into a machine for the first time or at unexpected hours.

Patch and Hunt. Patching is critical to preventing exploitation of existing vulnerabilities and subsequent remote compromise. After an infrastructure-wide vulnerability assessment and mitigation activity, engaging in penetration testing and hunting activities can further reveal potential weaknesses in the organization's security posture that could be exploited by actors with destructive intent.

Enact PowerShell Protections. IBM frequently observed threat actors leveraging PowerShell in malicious ways for their operations, including those launching destructive malware attacks. In recent cases we analyzed, PowerShell was used to download destructive payloads onto infected devices as well as to facilitate lateral movement. Monitoring PowerShell script use in the environment, restricting it where feasible, and alerting on unexpected PowerShell callouts can be valuable in detecting and preventing this type of activity.

Have backups, test backups, and keep offline backups. Backing up systems is a foundational best practice, but ensuring the organization has effective backups of critical systems and testing these backups is more important than ever and can make a difference in the case of any destructive malware attack on an organization.

Organizations of all sizes should store backups apart from their primary network and only allow read, not write, access to the backups. Offline backups are ideal, but for many organizations the cost and logistics preclude this option. X-Force IRIS's Christopher Scott notes that when considering how to configure backups, "you really have to think about the process. We have to have some rules that say: the backup system can access my primary network, but the primary network should not have access to my backup."

Those with responsibility for setting up backup systems should also ensure they are available not only in cases of fire, flood and earthquakes—disaster continuity—but that they are safe from the reach of attackers who may be searching for them internally.

Consider an action plan for quickly establishing a temporary business functionality. Organizations which have been able to restore even some business operations following a destructive attack have fared better than their counterparts. Organizations may want to consider developing a capability to set up a short-term, quick turnaround business function to allow continued operations while a destructive attack is being remediated. For example, organizations that have an alternate location and network for critical functions, have been able to continue critical business in the face of destructive malware attacks, even as remediation of or replacement of the original network is ongoing.

Where is destructive malware going next?

Based on data from our incident response teams, managed security services, and open source information, IBM X-Force IRIS assesses that destructive malware attacks are continuing to grow in popularity and effectiveness.

As we move into the second half of 2019, additional cybercriminal groups—particularly those intent on conducting ransomware attacks—are recognizing the utility of having a wiping mechanism built into their tools. This type of mechanism can provide adversaries with additional options to pressure victims, while simultaneously increasing the risk of an attack that will require disaster recovery. This trend leads us to believe that more financially-motivated cybercriminal groups are likely to explore destructive malware as an option to incorporate into current attacks, a task made easier when dark web markets provide these tools at relatively humble costs.

The year 2017 saw several ransomware attacks with destructive effects detrimentally affect numerous victims across the globe. While the number of victims and magnitude of damage from destructive ransomware has not yet reached these same levels in 2019, year-to-date trends suggest that the level of activity this year will be higher when compared to 2018.

In addition, 2017 attacks taught the world that just one critical vulnerability, if left unpatched, can be remotely and automatically exploited widely by malicious actors and cause widespread damage. We cannot discount the possibility that malicious actors could find and exploit a similar vulnerability in the future, causing additional widespread destruction.

Most groups carrying out destructive malware attacks today are sophisticated, stealthy, and patient, using advanced TTPs to infiltrate networks, and going to great lengths to cover their tracks. These tactics suggest that, at least at present, destructive malware tends to lay in the hands of the most advanced cybercriminal groups or nation-state actors. However, if the popularity of these tools continues to grow, destructive malware capabilities may become a reality for groups we tend to associate with lower levels of sophistication, such as some hacktivist groups or even terrorists.

In terms of geographical focus, we anticipate that the effects of destructive malware attacks are likely to grow. For example, targets located in the United States and Europe are increasingly falling victim to destructive malware attacks using destructive ransomware such as LockerGoga and MegaCortex. Destructive malware attacks in the Middle East and Asia are likely to continue, and have the potential to spread to other geographies as well. It is wise to prepare for the scenario of a destructive attack in all parts of the globe.

To keep up to date about attacks and adversarial TTPs, please join us on X-Force Exchange.
Check out X-Force Exchange

To learn more about X-Force IRIS, check out our IBM Security home page.
Check out the home page

If your team is already looking to test its response skills, contact IBM X-Force Command Center cyber ranges and come train with the world's premier cyber special forces team in a fully immersive attack scenario that we will tailor to your specific needs.
Check out the X-Force Command Center

If your organization believes it might be under attack, please contact our IBM X-Force Emergency Response Hotline at: 1-888-241-9812.

IBM Security

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations stop threats, prove compliance, and grow securely.

IBM operates one of the broadest and deepest security research, development and delivery organizations. It monitors more than two trillion events per month in more than 130 security patents. To learn more, visit ibm.com/security

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
August 2019.