Global Threat Intelligence Center

Monthly Threat Report

January 2021

Contents

Endpoint device evasive attack stages

Lead Analyst: Terrence Lillard, Principal DFIR Consultant, US

To assist organizations which have been compromised, the Digital Forensics and Incident Response (DFIR) Team responds to breaches at client environments. Part of that tasking is to help clients mitigate and recover from breaches. This includes analyzing the root cause of the breach.

The global threat landscape has evolved greatly over the past few years. In the past, organizations primarily implemented security controls to prevent attackers from penetrating their organization's applications or network perimeter devices. This approach was principally based on attackers exploiting vulnerable applications, devices or protocols. While attackers are still widely using those attack techniques, today's attackers are also commonly using more evasive attack techniques to bypass perimeter security controls (e.g., firewalls) organizations have implemented.

What is an evasive attack technique?

Evasive attack techniques are malicious activities not prevented or detected by standard security controls implemented within organizations. Many of these attacks occur on end user systems (e.g., Microsoft Windows 10), within an organization through users reading malicious email messages (e.g., phishing), downloading documents from malicious or compromised websites (exploit kits and hostile websites), or attackers accessing endpoint devices via vulnerable remote access applications (Remote Desktop Protocol). Attackers extend attacks by spreading laterally through the organization and outwardly to the internet. These attacks, which typically originate on endpoint devices, occur in four stages (Figure 1). The actual attack can be conducted with a variety of techniques, but ultimately, successful attacks tend to adhere to all four stages:

Evasive attack techniques

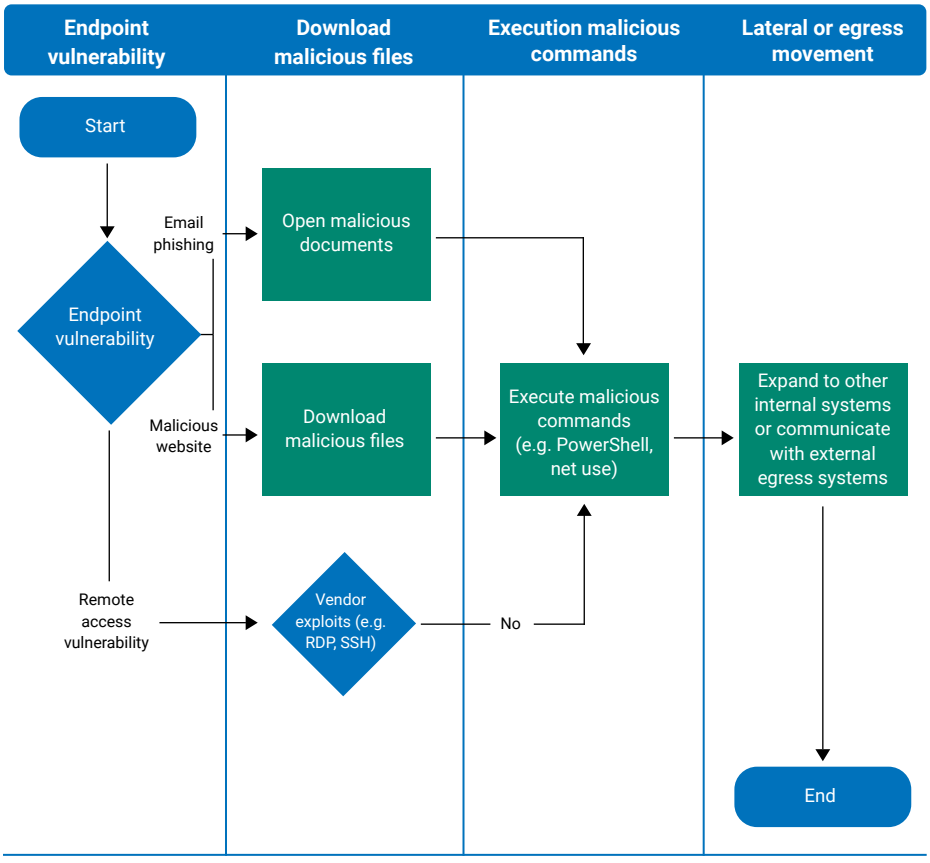

Figure 1: Stages of an effective evasive attack

The four stages of an effective evasive attack

- In the first stage, **Endpoint vulnerability**, an attacker identifies a vector to obtain access to an organization's endpoint device. This is often via malicious email messages, browsing malicious or compromised websites, or the attacker exploits remote access vulnerabilities. During this stage, the attacker often convinces a user to perform an action on a malicious email message or to download a file from a malicious or compromised website. In addition, the attacker can obtain access to an endpoint device by directly exploiting a vulnerable remote access application (e.g., RDP, SSH).
- In the second stage, **Download malicious files**, an attacker uses an end-point user system to establish an outbound connection to an external website and download malicious files (which contain commands, tools or scripts). Because the actions are originated from an internal user, and typically are not overtly hostile, the organization's security controls do not usually prevent or detect the files from being downloaded.
- In the third stage, **Execution of commands**, an attacker uses established remote access or convinces the user to execute commands in the file which are native to the operating system (e.g., PowerShell, Net Use, Schedule Task), or which do not generate antivirus signature alerts (MimiKatz, CobaltStrike). Commands native to the operating system are referred to as Living-off-the-Land Binaries (LOTLBins).
- In the final stage, **Lateral or egress movement**, an attacker identifies and compromises other devices within the organization. The attacker uses information obtained from the previous stages (e.g., passwords, hostnames, IP addresses) and launches attack techniques to compromise other host devices. An attacker is typically seeking servers (e.g., file servers, application servers, database servers, domain controllers) to compromise. The attacker also takes advantage of internal vulnerabilities and trust relationships with the compromised workstation.

Every organization has their own data, business needs, staff, priorities, policies, procedures and practices. **But most of the evasive breaches are not so unique.**

What can you do to prevent this?

When it comes to compromising details, every organization is different. Every organization has their own data, their own business needs, their own staff, priorities, policies, procedures and practices. But ultimately, most of the evasive breaches, and what makes such attacks successful in an organization's environment, are not so unique. If we consider the things clients can do to reduce the chances of an evasive breach, or to reduce the damage of such an attack, we can probably isolate most (not all) of the problems to five areas of control.

1. **User awareness and education**
   Phishing attacks are the single biggest source of incident engagements in client environments. Analysis for previous editions of NTT's Global Threat Intelligence Report revealed that it as much as 78% of malware enters client environments through phishing attacks. Phishing attacks introduce malware, often through malicious attachments in PDF and document formats. They also deliver redirects or links which lead to exploit kits. Attackers use these techniques to establish an initial foothold on workstations in the targeted client environment.

   Effective user awareness and education can reduce the chances of users opening malicious documents and clicking on malicious web links and can increase the effectiveness of the response.
2. **Limit the attacker's ability to Living-off-the-Land (LOTLBins)**
   Attackers regularly take advantage of commands, software and tools (e.g., PowerShell, Schedule Tasks, Net Use) already in the targeted environment. An organization can help limit this by reducing users' administrative access to their endpoint devices. Organizations can also disable or remove access to tools, especially remote access tools, which the organization is not using as a normal course of operations or support.

   Additionally, an organization can help by implementing an effective access control framework which regulates who or what can view or use resources in a computing environment – further limiting access to privileged data and tools.
3. **Minimize privilege escalation**
   Attackers aggressively work to extend their access to administrative or privileged accounts to increase their access within the organizational environment. They do this by using malicious software to capture administrative and privilege account passwords. An organization can help minimize this by barring administrators from performing routine work functions like reading email and browsing the web with their administrative account – they should be required to use 'user-level' accounts.

Additionally, an organization can help identify attempts by monitoring administrative and privilege account activity.

4. **Restrict lateral or egress movement**
   An attacker's next objective is to expand their foothold by attacking other systems within the organization, targeting servers and domain controllers to maximize their access.

   An organization can interfere with this process by monitoring server and file access and modification activity. An organization can further limit lateral or egress movement by implementing firewall restrictions to prevent or reduce server inbound and outbound connections.

   Additionally, attackers often take advantage of internal vulnerabilities to conduct lateral movement. Organizations should include internal patches and upgrades in their patch management program, specifically including patches for EternalBlue (MS17-010).

5. **Breach and incident response management**
   Regardless of exactly what the attacker is doing in the organizational environment, the faster an organization can detect and respond in an effective manner, the better. Organizations should actively monitor and test their internal environment to ensure internal controls are functioning correctly and increase the chances they can identify failures. This includes monitoring for exfiltration of internal information and connections to known or suspected command and control sites.

   Organizations can also use penetration tests to help identify potential vulnerabilities and exposed systems in a proactive manner.

   Additionally, organizations must have an effective Incident Response Plan, as well as train staff on the plan and test the plan.

Summary

Giving a tidy bullet list does not necessarily make the process dramatically easier. It is hard for any organization to suddenly reprioritize their security initiatives in directions they had not anticipated. But, all these security controls can help an organization become more resilient, better prepared to withstand an evasive attack or at least to manage it. Even if your organization can't do everything, it is worth considering which of these steps you can take to move your organization forward to mitigate evasive attack techniques.

Security controls help organizations become more resilient, better prepared to withstand evasive attacks - or at least manage them.

#Spotlight 1

Securing patient outcomes

Lead Analyst: Haydn Bowers, Security Solutions Architect, NTT Ltd., Australia

Trends, lessons and recommendations from the 2020 HIMSS Security Forum

The development of patient-centric care is leading a digital transformation within the healthcare industry. The first phase looks to the digitization of the hospital, with electronic health records (EHR), real-time location services and the messaging integration services replacing paper, faxing and paging. As the health industry adopts greater interoperability, patient care continues to diversify. This includes not just delivering acute hospital-based care but also care at home; and then further still to preventive and proactive care with the use of Internet of Medical Things (IoMT), such as wearable technology, like your smartwatch. The changing dynamic between patient and health provider is creating new challenges for security teams. Delivering healthcare to the patient, at home, via Telehealth or collecting data through IoMT, alters the attack surface along with the responsibility of health services to secure the many ways patients want to receive care.

Based on discussions at the 2020 Healthcare Information Management Systems Society Security Conference, balancing functionality, usability and security in healthcare is unique. Research demonstrates that misaligned security controls can detrimentally affect patient care, where timelines are measured in seconds and the impacts are patient outcomes. It is within this clinical context that healthcare security programs are beginning to consider the following recommendations to effectively embed security within the organization.

1. **Align cyber-risk with clinical risk**
   Cybersecurity teams need to understand the clinical service catalogue and criticality of services, for example, the criticality of ambulatory, mental health, allied health or research to the organization. With the establishment of a health service catalogue, the underlying applications and infrastructure which support these services can be secured with proportionate controls.
2. **Simplify identity and access management**
   Logging-in and on/off-boarding needs to be seamless for clinicians, where having to remember complex passwords and use multifactor authentication may distract clinicians from the task at hand. Additionally, identity is more nuanced in healthcare as clinicians have different roles throughout the day. For example, the ability to access and authorize the provision of medication may not lie with the same individual across an entire shift. The capability to implement least-privileged access needs to be flexible and easily provisioned by staff on the ground, akin to a nurse unit manager.
3. **Innovate to cloud-based security**
   Clinicians increasingly deliver care via Telehealth and in the home, while looking to tele-medicine, and innovate towards proactive and preventative care with IoMT and home monitoring. Health services will look to the cloud to manage such diversely delivered services. Security programs need to follow suit, securing the future, securing how patients want to receive care. Security technologies which should be considered include cloud-based antivirus and endpoint detection and response (EDR) for remote clinicians, cloud-proxy and secure-access-service-edge (SASE) for IoMT and remote access, cloud workload protection (CWP) and cloud-access security brokerage (CASB) as organizations use Big Data to analyse patient information.

Cybersecurity and privacy programs must enable health services to simplify their processes and innovate across the entire organization. Seamless, integrated and automated information security practices differentiate health services, increasing the business-value of the provider.

For healthcare, security is not just a data protection issue, it is a patient safety issue. The success of a healthcare security program should correlate to improved patient outcomes.

> Security is not just a data protection issue, **it is a patient safety issue.**

The fight to secure distributed working **is far from over**

Lead Analyst: Richard Thurston, Market Insights Manager, Strategy & Alliances, NTT Ltd., UK&I

The shift to distributed working, accelerated by the pandemic, continues to disrupt organizations' attempts to mitigate risk.

In a 2020 whitepaper for NTT, authored by technology industry analyst Omdia, the published data demonstrated that five out of six organizations were not fully prepared to move to remote working. Thirty-four percent hadn't even considered remote working until the pandemic struck.

The impact for many organizations has been seismic, as security teams grapple with the implications of shadow IT, the rapidly evolving threat landscape and updating organization-wide policies.

Our workplace research found that a substantial 83.3% of organizations have needed to completely re-think their IT security to accommodate new ways of working brought about by the pandemic (the manufacturing sector has been hardest hit, dogged by a larger proportion of on-site workforces and lower prior levels of digitalization).

Despite advances with vaccines, these issues won't be diminishing soon: less than half of organizations (43.1%) are planning to return to the working environments they had prior to the pandemic, so organizations must continue to acquire tools and update processes to support their new working model.

There is a long way to go. Worryingly, only 51.7% of organizations reported updating their remote working policies in the first four months of the pandemic, according to our research. Fewer (46.4%) increased their security tools.

And there is some evidence of scarce security skills being side-tracked; nearly half (47%) of cybersecurity professionals say they've been distracted from some or all of their day job to help with other tasks, such as providing the remote workforce with IT equipment, according to certification provider (ISC).

These distractions can only be detrimental to a strong cybersecurity posture, which remains – on average – well short of organizations' targets, as shown in our 2020 Global Threat Intelligence Report.

The Chartered Institute of Information Security stresses the urgency for everyone in organizations to know how to apply cybersecurity good practice (even at home, where employees may be more complacent and/or feel a false sense of security), and emphasizes the importance of security teams embedding these practices as a top priority while the world emerges from the pandemic and distributed working models evolve in response.

It is worth pointing out that workplace concerns are about more than distributed working. Omdia wrote in its whitepaper that CISOs will want to address a raft of remaining resilience questions given further potential shocks.

2021 may be the year the world starts to overcome a health pandemic, but the effects on how work is undertaken and the consequent evolution of threats to organizations' information assets have not yet been fully felt.

Nearly half of responding cybersecurity professionals say they've been distracted from some or all of their day job to help with other tasks such as providing the remote workforce with IT equipment.

NTT's Global Threat Intelligence Center

The NTT Global Threat Intelligence Center (GTIC) protects, informs and educates NTT Group clients through the following activities:

- threat research
- vulnerability research
- intelligence fusion and analytics
- communication to NTT Group clients

The GTIC goes above and beyond the traditional pure research organization, by taking their threat and vulnerability research and combining it with their detective technologies development to produce applied threat intelligence. The GTIC's mission is to protect clients by providing advanced threat research and security intelligence to enable NTT to prevent, detect and respond to cyberthreats.

Leveraging intelligence capabilities and resources from around the world, NTT's threat research is focused on gaining understanding and insight into the various threat actors, exploit tools and malware – and the techniques, tactics and procedures (TTP) used by attackers.

Vulnerability research pre-emptively uncovers zero-day vulnerabilities that are likely to become the newest attack vector, while maintaining a deep understanding of published vulnerabilities.

With this knowledge, NTT's security monitoring services can more accurately identify malicious activity that is 'on-target' to NTT Group clients' infrastructure.

Intelligence fusion and analytics is where it all comes together. The GTIC continually monitors the global threat landscape for new and emerging threats using our global internet infrastructure, clouds and data centers along with third-party intelligence feeds; and works to understand, analyse, curate and enrich those threats using advanced analysis techniques and proprietary tools; and publishes and curates them using the Global Threat Intelligence Platform (GTIP) for the benefit of NTT Group clients.

Our **Global Threat Intelligence Center** goes beyond a traditional research-only approach by combining focused research with detective technologies. This results in **true applied threat intelligence** to protect our clients with effective tools and services which reduce security risks and threats.

Recent assets

2020 Global Threat Intelligence Report

Our 2020 Global Threat Intelligence Report (GTIR) is the culmination of the data the Global Threat Intelligence Center gathered and analyzed throughout the year. We produce this report by collecting a broad set of global data (log, event, attack, incident and vulnerability) to identify key cybersecurity trends of which businesses need to be aware.

Download report

If you haven't already, **register to receive the Monthly Threat Reports** directly to your inbox each month.


NTT