Symantec by Broadcom

WHITE PAPER

Abuse of Trust: A New Trend in Targeted Attacks?

How social engineering, phishing, and security weaknesses can provide attackers with deep access to corporate networks.

By the Symantec® Threat Hunter Team

WHITE PAPER

Abuse of Trust: A New Trend in Targeted Attacks?

Symantec by Broadcom

TABLE OF CONTENTS

Introduction

One of the most significant macro trends in malicious cyber activity in recent years has been the steady reduction in reliance on malware by attackers. While malicious tools often represent the quickest and easiest way to mount an attack, their use does come with a price. Malware is conspicuous, and increasingly so as modern security solutions improve. Malware authors now need to work much harder to evade detection, and once the malware is discovered, its value immediately diminishes. Malware authors now have to work harder for diminishing results.

This environment has led attackers to look at alternative tools, tactics, and procedures (TTPs), with the most significant development being a switch to legitimate tools. The right combination of legitimate tools in the hands of an attacker can often work as well, if not better, than malware.

Legitimate tool usage can be split into two broad categories: dual-use tools and living-off-the-land. Dual-use tools are legitimate software packages that can be used for malicious purposes by attackers who introduce them onto the victim's network. Living-off-the-land refers to the tactic of attackers utilizing tools that are already installed or available on the target's network. In many cases, this tactic involves the use of operating system features and network administration tools.

The appeal of legitimate tooling for attackers is obvious, as it provides them with an opportunity to be undetected. A legitimate tool is less likely to raise suspicions and be less likely to trigger an antivirus detection. Malicious activity becomes hard to detect, hidden within the vast amount of legitimate activity on the victim's network.

While the shift to legitimate tools certainly benefited attackers, the advantages they bestow are steadily diminishing as security software and network defenders continually hone their ability to identify and block this malicious activity. This will lead attackers to search for new and more effective TTPs. Several possibilities exist as to what the next major tactical evolution might be, but one possibility lies in the growing number of attacks that involve little to no tool usage. These *tool-free* attacks instead rely on obtaining access to targeted networks by other means, particularly through the acquisition of valid credentials.

Tool-free tactics have, to date, been used by a small number of actors (although individual elements have been used far more broadly). Attacks share a number of broad characteristics:

- Adept use of social engineering
- An in-depth knowledge of enterprise software and systems
- Knowledge of working practices and workflows
- An ability to identify and exploit security weaknesses and lapses, such as improperly configured cloud storage or credentials stored in code
- Recruiting of insiders within a target organization

Whether these tactics emerge as the next major threat remains to be seen. Nevertheless, organizations should heed the lessons learned from their use to date.

Early Usage: SIM Swapping

Perhaps one of the earliest examples of these tactics is so-called *SIM swapping* attacks, where attackers rely on social engineering alone to bypass multi-factor authentication (MFA) systems. A large number of MFA systems utilize the end-user's cell phone to authenticate login requests. For example, someone attempting to log in to their bank account online may be asked to authenticate that request either through a mobile app or by receiving an authentication code through SMS.

Generally speaking, SIM swapping might be the last step or *the missing puzzle piece* for an attacker to obtain full access to their target's account. They might have already bought their data on the cyber underground from attackers selling breached data, and they could potentially supplement that data with open-source information. This stolen data might sometimes give the attackers enough information to create a convincing SIM swapping attack, that is, they know enough about the target to masquerade as them.

MFA Fatigue Attacks

SIM swapping is most effective against MFA solutions that use SMS. Most MFA solutions contain safeguards that make it more difficult to bypass them than simply swapping a SIM card. However, attackers have found other MFA bypass techniques, most significantly so-called MFA Fatigue attacks.

The tactic is quite simple. Many MFA systems operate by pushing a notification to the user's mobile device after a login is attempted. The user then confirms or denies the login request. Attackers can repeatedly attempt to log in to a user's account with stolen credentials, generating multiple push notifications in the hope that the user might inadvertently confirm one.

If the target fails to fall for this, the attackers might decide to apply additional pressure by either emailing or calling the victim to lure them into accepting a request. For example, the attackers might pretend to work for the target's IT department and say they need to approve the request in order to perform some routine maintenance on their account.

Social Engineering Component in Ransomware Attacks

Some of the largest cyber-crime groups have begun to recognize the effectiveness of these tactics and integrate them into their attack chains. One example is the Miner (also known as Wizard Spider) cyber-crime group, which has been responsible for a range of banking Trojans (for example, Dyre and Trickbot) and ransomware operations (for example, Ryuk and Conti). In some ransomware attacks carried out by affiliates of the group, it has employed its own call center (dubbed BazarCall) to lure victims into installing malware.

For example, in a campaign targeting a number of large organizations during July 2021, a spear-phishing email was sent to selected employees. The email alleged that the recipient had been involved in a recent car accident and a claim had been made against their motor insurance. They were given a number to call for further information. The email was convincing enough for the employee to call the number. The subsequent phone call directed them to a URL. This URL led to the download of a malicious Excel file that, when opened, installed malware onto the unsuspecting victim's machine.

The tactic of using a phone call to get the target to download a suspicious file was a bid to avoid detection. A suspicious attachment or link in an email from an unknown sender is likely to either be automatically blocked by security software or raise the suspicions of the recipient. A URL that is manually entered by an end-user might not be as likely to generate a warning. Using this technique in social engineering helped the attackers to achieve what malware could not, and it led to at least one employee downloading a malicious file.

Emerging Trend in Espionage Attacks

The Fritillary group (also known as APT29 and Cozy Bear) is one of the more active and long-established Russian-sponsored espionage groups. Multiple governments, including the U.S., UK, and Canada believe that the group is a unit of Russian Foreign Intelligence.

Fritillary has been active since 2010, and it is known to target high-profile individuals and organizations in government, international affairs, policy and research. It has been particularly active against diplomatic organizations in the U.S. and Europe. The group has been linked to some of the most ambitious and impactful Russian-sponsored attacks in recent years. In 2016, Fritillary along with another Russian-sponsored group Swallowtail, was implicated in the cyber attacks that preceded the U.S. presidential election.

According to the Department of Homeland Security and the Federal Bureau of Investigation (FBI), in the summer of 2015, the group was responsible for sending spear-phishing emails to over 1000 targeted individuals, including some U.S. government personnel. These emails contained malicious links that, if clicked, would lead to unnamed malware being installed on the target's computer. This malware allowed the attackers to compromise a political party's systems and steal emails from several accounts on the network.

In late 2020, Fritillary was linked to the SolarWinds software supply chain attack, one of the most ambitious and sophisticated software supply chain attacks ever mounted. The compromise provided the group with access to thousands of organizations, allowing it to cherry-pick targets of interest for further intrusions.

In order to carry out the attack, Fritillary gained access to the software build process for SolarWinds Orion, infrastructure monitoring and management software that is widely used by large enterprises. It then modified a legitimate code library, which allowed it to deliver a backdoor Trojan known as Sunburst (Backdoor.Sunburst) to any Orion user who downloaded an update to the software during a nine-month period.

This supply chain attack provided Fritillary with a foothold onto the networks of an estimated 18,000 organizations worldwide. However, only a small subset of organizations were selected for further malicious activity, suggesting that these were organizations of interest to the attackers and that the vast majority of victims were considered collateral damage from a wide-scale trawl.

In these targeted organizations, additional pieces of custom malware known as Teardrop (Backdoor.Teardrop) and Raindrop (Backdoor.Raindrop) were deployed. Both pieces of malware acted as droppers delivering the final payload for these attacks, commodity malware known as Cobalt Strike.

In April 2021, the U.S. government formally attributed the SolarWinds attack to Fritillary.

Shift to Tool-Free Attacks

While Fritillary has been adept at the development and deployment of custom malware, the group is showing a marked shift away from malware development.

The most notable example of this shift is a campaign documented by Mandiant in August 2022, which involved repeated targeting of Microsoft 365 users in a number of NATO countries. The attacks were reported to be largely focused on organizations involved in foreign policy.

A key obstacle in carrying out attacks was MFA in Azure Active Directory and other services. Fritillary discovered a potential workaround for MFA through the fact that most platforms permit users to enroll their first MFA device at login. By guessing the passwords to unused or dormant mailboxes, the group was able to enroll its own devices for MFA and then use these compromised accounts to log in to the target's VPN.

One of the biggest challenges in accessing Microsoft 365 accounts is that evidence of such access is likely to be logged. Logging tools present a challenge to attackers. One such tool is Purview Audit, formerly known as Advanced Audit, which is made available to Microsoft 365 customers with E5 licenses. Purview Audit logs the user-agent string, timestamp, IP address, and user for each instance a mail item is accessed. It can potentially provide evidence of a breach and also give incident response investigators some evidence as to who the attacker might be. Consequently, disabling Purview Audit was one of the first steps Fritillary took after gaining access to a user's account, allowing it to cover its tracks to a certain extent.

In one case, the attackers managed to obtain access to an administrator account in Azure AD. They leveraged this account to impersonate an application's service principal object in Azure to add a new certificate. This certificate allowed them to authenticate themselves in Azure AD and begin harvesting emails from selected mailboxes. To avoid raising suspicions, the certificate was created with a name that matched the display name of the service principal.

A feature of the attacks was the level of operational security employed. Fritillary used Azure virtual machines (VMs) to access the targeted networks. These VMs belonged to Azure accounts outside of the targeted organization and might have been previously compromised or purchased surreptitiously by the attackers. The attackers likely chose to do this because Microsoft IP addresses might be less likely to raise suspicions.

No malware appears to have been used in this campaign. Aside from the level of caution employed in maintaining operational security, what is striking is the sheer depth of knowledge displayed by the attackers about the systems involved in order to successfully exploit relatively limited weaknesses in their targets' security postures.

Lapsus$: A New Template for Network Intrusions

In early 2022, a new threat actor appeared on the scene that very quickly made a name for itself due to successful intrusions of a number of high-profile organizations leading to the theft of internal data and intellectual property.

Calling itself Lapsus$, the group appeared to be a loose collective of disparate individuals spread across multiple countries. Initially seen as an extortion gang, Lapsus$ appeared to be even more interested in gaining notoriety and embarrassing its victims.

While Lapsus$ might never have intended to establish itself as a serious cyber-crime player, its arrival is nevertheless noteworthy due to the novel TTPs it deployed. Their TTPs effectively sketched out a potentially new attack model for extortion actors. Lapsus$ made only limited use of malware and dual-use tools. Instead, through a combination of phishing, social engineering, and an apparently in-depth knowledge of corporate systems and working practices, it managed to stage highly successful intrusions against its targets.

Early Attacks

While the group claimed responsibility for a number of earlier attacks against Portuguese-speaking organizations, such as the compromise of Portuguese media company Impresa, Lapsus$ first came to significant public attention with an attack on chip-making giant Nvidia. It claimed to have stolen approximately 1 TB of data from the company, including credentials belonging to some 71,000 employees, which it promptly posted online. An early indication that Lapsus$ might not be the traditional financially motivated threat actor came with its ransom demand. Instead of asking for money, it threatened to release the remaining stolen data unless Nvidia removed lite hash rate (LHR) limitations from GeForce RTX 30 Series firmware. It also demanded that Nvidia commit to open-sourcing its GPU drivers for Windows, macOS, and Linux devices.

The group then demonstrated that the Nvidia breach was not a chance attack when it took credit for an attack on electronics manufacturer Samsung, leaking a huge trove of data it claimed to have stolen from the company.

Lapsus$ said the leak contained *confidential Samsung source code* that was stolen in a breach. According to Lapsus$, the leak included source code for every trusted applet installed in Samsung's TrustZone environment used for sensitive operations (for example, hardware cryptography, binary encryption, access control); algorithms for all biometric unlock operations; bootloader source code for all recent Samsung devices; source code for Samsung's activation servers; and full source code for technology used for authorizing and authenticating Samsung accounts, including APIs and services.

Microsoft Intrusion

In March 2022, Lapsus$ attacked Microsoft and claimed that it had accessed the company's internal DevOps environment, sharing screenshots of what it claimed to be Microsoft engineering projects. It followed up this announcement by releasing an archive with what it claimed was source code from Bing, Bing Maps, and Cortana.

Microsoft's subsequent report on the group's activities shed significant light on how Lapsus$ was carrying out its attacks.

The group made heavy use of social engineering tactics but would also use some malware and living-off-the-land tools once they gained access to a network. They used the following range of tactics to gain initial access:

- Purchasing credentials or session tokens on underground forums
- Paying employees for access to credentials and MFA
- SIM swapping to facilitate account takeover
- Accessing employees' personal accounts to retrieve any useful information or credentials
- Using the Redline password stealer to retrieve credentials and session tokens
- Searching public code repositories for exposed credentials

Lapsus$ attacks were often successful because the group gained *intimate* knowledge of a target's employees, systems, and processes.

Once inside a network, the group used a wide range of TTPs to elevate privileges, move laterally, and obtain data. Their TTPs included the following items:

- Exploiting unpatched vulnerabilities on internal servers including JIRA, Gitlab, and Confluence
- Searching code repositories and collaboration platforms for exposed credentials and other confidential information
- Using AD Explorer, a publicly available tool to enumerate users and groups
- Mining collaboration platforms such as Slack or Teams to obtain useful information
- Using DCSync attacks and Mimikatz to obtain credentials
- Social engineering calls to internal help desks

In some cases, the group has even managed to join internal crisis communication calls to understand incident response workflows.

In order to exfiltrate data, Lapsus$ had its own dedicated infrastructure in known virtual private server providers and uses NordVPN for its egress points.

Microsoft acknowledged that it had been breached, but said only a single account had been compromised, *granting limited access*. While the attackers used some of the TTPs mentioned in the report, Microsoft did not elaborate on the specifics.

Subsequent Attacks

The group staged a number of other intrusions after the Microsoft attack, including one against authentication provider Okta. In a statement, Okta announced that around 2.5% of customers had potentially been impacted, meaning their data *might have been viewed or acted upon*.

The breach was confined to the compromise of the account of a third-party customer support engineer working for one of Okta's contractors (Sitel). There was a five-day window before the compromise was discovered where the attackers had access to the Sitel environment.

In April 2022, T-Mobile confirmed reports that Lapsus$ had gained access to its systems several weeks previously. The confirmation came after Brian Krebs obtained access to the internal chats of core Lapsus$ members. The chats appeared to show that Lapsus$ had access to several T-Mobile systems, including a tool the company used to manage customer accounts.

Lapsus$ stated that it gained access to T-Mobile through VPN credentials the group purchased on a hacking forum. The gang said it targeted T-Mobile because it would help them conduct SIM swapping attacks.

"The systems accessed contained no customer or government information or other similarly sensitive information, and we have no evidence that the intruder was able to obtain anything of value," T-Mobile said. "Our systems and processes worked as designed, the intrusion was rapidly shut down and closed off, and the compromised credentials used were rendered obsolete."

In September 2022, transport and delivery firm Uber said that Lapsus$ was behind a breach in which the attackers managed to access a wide range of company systems and post obscene images on internal communications channels. The attackers gained access to the company's network by obtaining an employee's credentials and succeeded in getting them to accept a two-factor authentication (2FA) request.

"From there, the attacker accessed several other employee accounts which ultimately gave the attacker elevated permissions to a number of tools, including G-Suite and Slack," Uber said. "The attacker then posted a message to a company-wide Slack channel, which many of you saw, and reconfigured Uber's OpenDNS to display a graphic image to employees on some internal sites."

The person who claims to have carried out the attack said that he was 18 years-old and shared evidence of his intrusion with The New York Times, including *images of email, cloud storage, and code repositories*.

Impact and Aftermath

The group's novel tactics, its desire for notoriety, and a minimal interest in profit meant that Lapsus$ was an unpredictable actor with a penchant for creating chaos. An early example of this behavior was the theft of digital certificates during the Nvidia breach. The group then leaked these certificates, which were subsequently used to sign malware. Shortly after news of the leaked certificates emerged, security researchers found them being used on several pieces of malware that were uploaded to the malware scanning service VirusTotal. This malware included variants of Cobalt Strike beacon, the credential-dumping tool Mimikatz, and a number of backdoors and remote access Trojans (RATs).

Instead of using the usual channel of a darknet page to leak stolen data, the group's main communications channel with the rest of the world was Telegram. It would post the data stolen from breached organizations and even run polls on whose data it would leak next.

However, the group's very public activity was probably ultimately the source of its downfall as police began to identify suspects and make arrests shortly after it first came to prominence. In March 2022, police in the UK announced that they had arrested seven people, between the ages of 16 and 21 in connection with the attacks. Two of those arrested were subsequently charged.

In October 2022, Federal Police in Brazil arrested a suspected member of the group. The arrest was made in the Brazilian city of Feira de Santana. While few details about the individual were disclosed, police officials said they were being charged with crimes related to operating a criminal organization, invasion of computer devices, technological disturbances, and more.

Such was the impact of the attacks that in December 2022, the U.S. Department of Homeland Security Cyber Safety Review Board (CSRB) announced that it was investigating attacks attributed to Lapsus$. The goal of the CSRB's review of the gang's activities was to provide advice on defending against Lapsus$ attacks. "The CSRB will review the cyber activity of Lapsus$ in order to analyze their tactics and help organizations of all sizes protect themselves," CSRB Deputy Chair Heather Adkins said.

A number of alleged Lapsus$ members were arrested earlier this year. Most of this group's members are believed to be teenagers carrying out attacks in order to make a name for themselves on the hacking scene.

Key Lessons

The attacks by Lapsus$ and Fritillary discussed previously represent the most comprehensive use to date of tool-free tactics. The success of these attacks highlight the following priorities for any organization wishing to guard against similar tactics:

- **Credentials:** A key component in tool-free attacks is the use of stolen or guessed credentials. Organizations should have a rigid credential security policy that obliges employees to not only select highly secure passwords but also to regularly change those passwords. Employees should be educated on the importance of password security and strongly discouraged from re-using, sharing, or improperly storing passwords. Dormant or unused accounts should be regularly audited and removed if not required.
- **MFA:** Organizations need to be aware of the limitations or potential weaknesses in some MFA solutions. For example, 2FA can in some cases be bypassed, particularly if the target is using SMS-based 2FA, through the use of SIM swapping attacks. While most MFA solutions are more robust than this, attackers might still attempt to enroll their own devices. For example, by taking advantage of some policy loopholes where end-users can self-enroll the first device used with an account. However, there are other ways of bypassing MFA, such as MFA Fatigue attacks. MFA solutions should be configured to automatically block accounts where multiple requests are sent within a short space of time.
- **Social engineering:** Social engineering tactics can often be difficult to guard against, particularly if the attacker speaks the target's language fluently and displays a deep understanding of their business. Employee education is key, both in highlighting the resources some attackers have at hand (for example, call centers) and identifying some of the key tactics used to mount a convincing socially engineered attack. Clear security policies will help employees avoid finding themselves pressured or otherwise coerced into security lapses.
- **Public repositories:** While public code repositories are a useful resource, what is shared on these repositories needs to be carefully audited, since attackers will often hunt through uploads for inadvertent disclosures such as hardcoded credentials.
- **Cloud storage:** When used correctly, cloud services are highly robust. However, a leading cause of data breaches is when data is improperly secured on the cloud and in some cases, simply left publicly accessible to anyone who knows how to find it. Breached data can be used to extort organizations or can be leveraged to mount further attacks against the targeted organization.
- **Vulnerabilities:** The danger presented by exploitation of unpatched vulnerabilities is now well known. Organizations might understandably prioritize the patching of publicly facing systems. However, internal software should not be ignored, as there are cases of attackers exploiting vulnerabilities in internal systems once they have obtained access to a network through other means.

The combined use of these individual tactics is fairly new, and it remains to be seen if they truly gain traction. If entirely tool-free attacks do not become a phenomenon, components of those attacks seen to date will almost certainly be incorporated into the toolkits of some threat actors.

Mitigation

Symantec recommends that customers observe the following best practices to help protect against targeted attacks:

- **Local environment:**
  - Monitor the use of dual-use tools inside your network.
  - Ensure that you have the latest version of PowerShell and that you have logging enabled.
  - Restrict access to Remote Desktop Protocol (RDP) services. Only allow RDP from specific known IP addresses and ensure that you are using MFA.
  - Implement proper audit and control of administrative account usage. You could also implement one-time credentials for administrative work to help prevent theft and misuse of admin credentials.
  - Create profiles of usage for admin tools. Many of these tools are used by attackers to move laterally undetected through a network.
  - Use application allow listing where applicable.
  - Locking down PowerShell can increase security, for example with the constrained language mode.
  - Make credential dumping more difficult, for example, by enabling Credential Guard in Windows 10 or disabling SeDebugPrivilege.
  - MFA can help limit the usefulness of compromised credentials.
  - Create a plan to consider notification of outside parties. In order to ensure correct notification of required organizations, such as the FBI or other law enforcement authorities, be sure to have a plan in place to verify.
  - Create a *jump bag* with hard copies and archived soft copies of all critical administrative information. In order to protect against the compromise of the availability of this critical information, store it in a jump bag with the hardware and software needed to troubleshoot problems. Storing this information on the network is not helpful when network files are encrypted.
- **Email:**
  - Enable MFA to prevent the compromise of credentials during phishing attacks.
  - Harden security architecture around email systems to minimize the amount of spam that reaches end-user inboxes and ensure that you are following best practices for your email system, including the use of SPF and other defensive measures against phishing attacks.
- **Backup:**
  - Implement offsite storage of backup copies. Arrange for offsite storage of at least four weeks of weekly full and daily incremental backups.
  - Implement offline backups that are onsite. Make sure you have backups that are not connected to the network to prevent them from being encrypted by ransomware.
  - Verify and test your server-level backup solution. This should already be part of your Disaster Recovery process.
  - Secure the file-level permissions for backups and backup databases. Do not let your backups get encrypted.
  - Test your restore capability. Ensure that restore capabilities support the needs of the business.

Protection: How Symantec® Solutions can Help

Symantec® security solutions address today's security challenges and protect data and digital infrastructure from multifaceted threats. The following solutions include core capabilities designed to help organizations prevent and detect advanced attacks:

- **Symantec Endpoint Security Complete (SESC):** SESC was specifically created to help protect against advanced attacks. While many vendors offer Endpoint Detection and Response to help find intrusions, there are gaps. We call these gaps blind spots and there are technologies in SESC to eliminate them.

  LEARN MORE

- **Privileged Access Management (PAM):** PAM is designed to prevent security breaches by protecting sensitive administrative credentials, controlling privileged user access, proactively enforcing security policies, and monitoring and recording privileged user activity.

  LEARN MORE

- **Symantec Web Isolation:** Symantec Web Isolation eliminates web threats and solves the challenge of providing access to unknown, uncategorized, and potentially risky web sites by creating a remote execution environment between an agency's enterprise systems and content servers on the web.

  LEARN MORE

- **Symantec Secure Web Gateway (SWG):** SWG delivers a high-performance on-premises or cloud secure web gateway that organizations can leverage to control or block access to unknown, uncategorized, or high-risk web sites.

  LEARN MORE

- **Symantec Intelligence Services:** Symantec Intelligence Services leverages the Symantec Global Intelligence Network to deliver real-time threat intelligence to several Symantec network security solutions, including Symantec Secure Web Gateway, Symantec Content Analysis, Symantec Security Analytics, and more.

  LEARN MORE

- **Symantec Content Analysis with Advanced Sandboxing:** Within the Symantec Content Analysis platform, zero-day threats are automatically escalated and brokered to Symantec Malware Analysis with dynamic sandboxing for deep inspection and behavioral analysis of potential Advanced Persistent Threat files and toolkits.

  LEARN MORE

- **Symantec Security Analytics:** Symantec Security Analytics delivers enriched, full-packet capture for full network traffic analysis, advanced network forensics, anomaly detection, and real-time content inspection for all network traffic to arm incident responders for quick resolution.

  LEARN MORE

For more information, visit our website at: www.broadcom.com

AOT-NTA-WP100 June 27, 2023