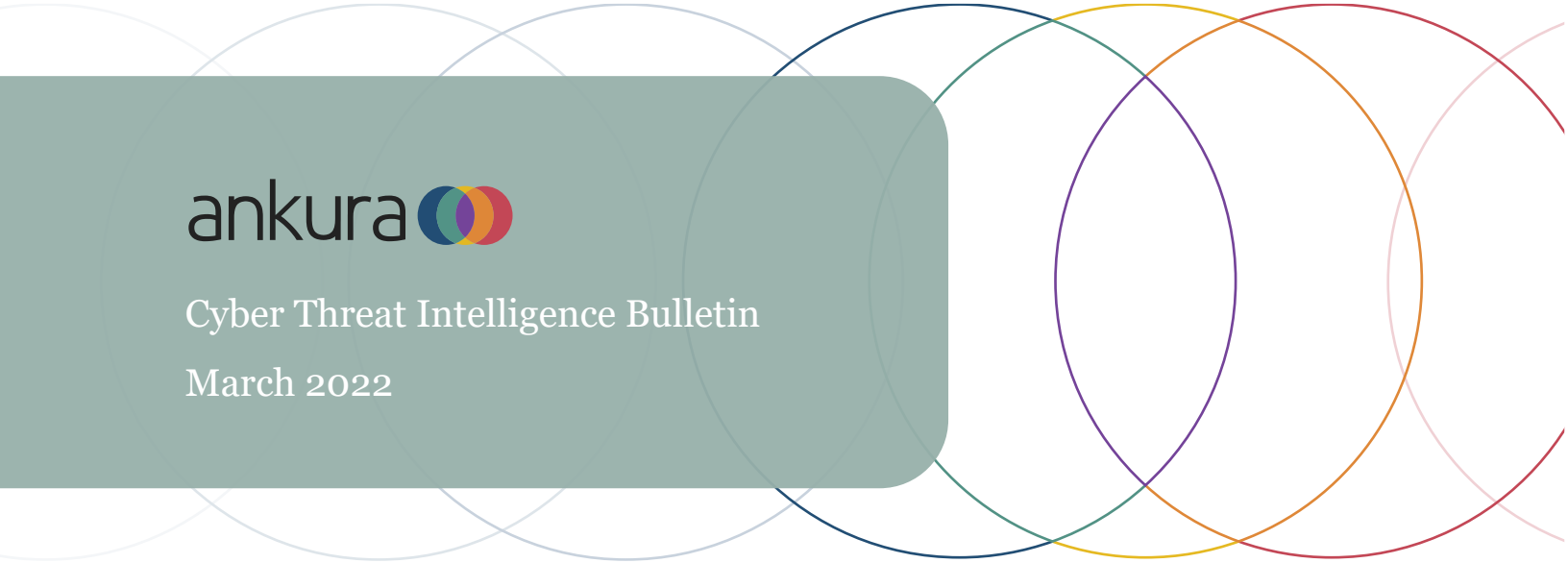


ankura

Cyber Threat Intelligence Bulletin

March 2022

Washington, DC
2000 K Street NW, 12th Floor
Washington, DC, United States 20006
+1.202.797.1111

Ankura Incident Response Services
Incident@ankura.com | 24/7 Assistance

TABLE OF CONTENTS

Executive Summary

Ankura's Cyber Threat Investigations and Expert Services (CTIX) team has compiled details of current cyber trends within the last sixty (60) days. This summary is intended to provide a medium depth of knowledge to high-level executives, technical analysts, and everyday readers who are looking to gain a deeper understanding of current, global threats.

This report will discuss the following in detail:

- Identification of newly uncovered features of the sophisticated malware "Daxin," which is being used by China-linked threat actors
- The emergence of two (2) successor sites in the wake of the March 2022 takedown of the hacking site "Raidforums"
- Chinese-backed nation-state threat group APT41 recently targeted United States state government entities by exploiting the Log4j vulnerability
- The tactics, techniques, and procedures (TTPs) of the Lapsus$ extortion group

A LOOK INSIDE THE DAXIN MALWARE

Key Points

- Highly sophisticated malware strain "Daxin" regains the spotlight through the recent analysis of its recent evolution.
- "Daxin" is attributed to Chinese state sponsored threat actor "OwlProxy" for the purpose of conducting sustained cyber espionage campaigns.
- Daxin bypasses firewall rules and evades detection by hijacking the network's existing TCP connections and listening for specific conditions dictated by the threat actors in order to establish an encrypted communication channel with command-and-control.

Summary

In early March of 2022, various reports began surfacing regarding recently uncovered features of Daxin, a known malware linked to Chinese advanced persistent threat (APT) actors. Daxin, otherwise known as "Backdoor.Daxin", is described as a "highly sophisticated piece of malware being used by China-linked threat actors" that has been "exhibiting previously unseen technical complexity and has been used in long-term espionage campaigns against specific governments and critical infrastructure organizations".[1] This malware allows threat actors to perform sophisticated data gathering and espionage operations against targets of strategic interest to China.

Daxin's sophistication is apparent in its capabilities to infect hardened targets without being detected. The malware is a Windows kernel driver that uses advanced communications functionality to remain undetected. Rather than starting its own network services, Daxin abuses legitimate TCP/IP services already running on the system, a technique known as "living off the land." To accomplish this, Daxin monitors all incoming TCP traffic for certain patterns and, when those conditions are fulfilled, Daxin disconnects the user and commandeers the connection. Next, it engages in a custom key exchange with the peer, opening an encrypted channel of communication for sending and receiving data and commands. Using this stealthy

[1] https://sensorstechforum.com/china-linked-daxin-backdoor/

method for network communication allows the threat actors to bypass firewall rules and evade detection by security operations center (SOC) analysts. Researchers have noted that one of Daxin's most interesting capabilities is to "create a new communications channel across multiple infected machines" using a single command to provide the list of nodes.[2] Some of Daxin's other capabilities include reading and writing arbitrary files as well as the functionality of starting and interacting with arbitrary processes.

Daxin's functionality can be extended by deploying additional modules on the victim's machine. The malware has the ability to provide a "dedicated communication mechanism for such components by implementing a device named \\.\Tcp4."[3] The components can then open \\.\Tcp4 to "register themselves for communication." Each module has the capability to associate a "32-bit service identifier with the opened "\\.\Tcp4" handle."[4] Once the identifiers are implemented, the remote threat actor is able to "communicate with selected components by specifying a matching service identified when sending messages of a certain type" and utilizes a mechanism to send back responses as well.[5]

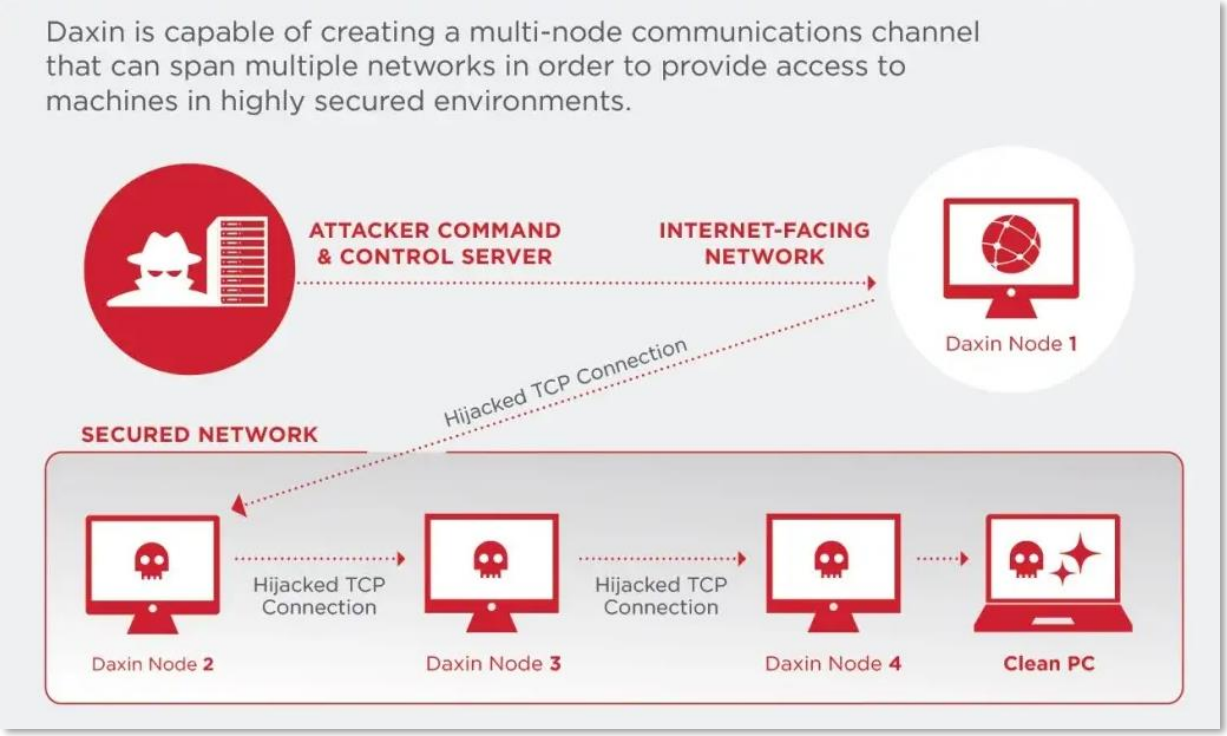


Figure 1: Breakdown of how Daxin creates communications channels to pivot through the infected system[6]

The Daxin backdoor has been linked to the Chinese state-backed hacking group "Owlproxy" (aka Slug/Chimera).[7] This piece of malware has been active in the wild since November of 2019. Signs of more significant attacks involving the deployment of the threat, however, were observed in May and July of 2020. The most recent attacks involving the distribution of Daxin were identified in November 2021 and targeted telecommunications, transportation, and manufacturing companies. It is speculated that a similar backdoor was first developed in 2013 (known as "Zala Backdoor" or "Win32/Exforel.A"), but the advanced detection-

[2] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/daxin-backdoor-espionage
[3] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/daxin-backdoor-espionage
[4] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/daxin-backdoor-espionage
[5] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/daxin-backdoor-espionage
[6] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/daxin-backdoor-espionage
[7] https://www.bleepingcomputer.com/news/security/more-hacking-groups-join-microsoft-exchange-attack-frenzy/

avoidance techniques and other functions were introduced later in development. It is believed that threat actors managed to evade detection and leveraged Zala Backdoor in their cyber espionage attacks long before the instances of the Daxin malware were detected in 2019. CTIX analysts will continue to monitor the activity of Chinese APT groups and their linked malware as they lurk in the shadows of trending global news.

WHAT HAPPENED TO RAIDFORUMS?

Key Points

- Raidforums, a popular hacking forum, was seized in late February 2022; as of publication, no public or private entity has claimed responsibility for the action
- Mass diaspora of users to a variety of other sites; in particular, two (2) main successors sites have been created thus far.

Summary

On February 25th, 2022, Raidforums, the popular hacking forum, was allegedly seized by an unknown entity. Raidforums is a well-known and historically stable host of database leaks, hacker groups, and general debauchery. Despite the seizing of the website occurring over one (1) month ago, there is still very little information revealed about who has taken possession of it. The seize was first confirmed by Raidforums admin "Jaw" who stated, "The raidforums.com domain has been seized. I encourage anybody that attempted logging in to change your passwords and clear any logs you have." The original Raidforums website appeared to then be used as a honeypot to try and scrape users' login information. Throughout late February and March, accusations have ranged from the Russian government to the United States Federal Bureau of Investigation (FBI) being responsible for this seizure. According to Databreaches.net, the FBI's response to questions regarding Raidforums was simply, "Thanks for reaching out. Decline to comment."[8]

The build up to the eventual seizing of Raidforums stems from January 30th, 2022, when connectivity issues started plaguing the forum. After returning to normal functionality on February 12th, 2022, the owner "Omnipotent" made no comment regarding the issues and the admins appeared to be unaware of what exactly had occurred.[9] Operability continued as normal until Jaw's announcement on February 25th, 2022, amid an abnormal event where all users were logged out of Raidforums and a new login page was created. Throughout the course of February, multiple events on Raidforums created interest and division. For example, a user known as "NetSec" was organizing multiple raids against United States-based entities around the same time as Raidforums admin "MOOT" declared a hard anti-Russia stance immediately following the onset of the invasion of Ukraine.[10] Due to multiple events concerning several world stage governments, it is difficult still to determine exactly what entity has taken over Raidforums at this time.

[8] https://www.databreaches.net/why-wont-law-enforcement-answer-questions-about-raid-forums-or-have-they-just-winked/
[9] https://securityboulevard.com/2022/03/raid-forums-is-down-whos-behind-its-apparent-seizure/
[10] https://blog.cyble.com/2022/03/03/ongoing-cyberwarfare-2/

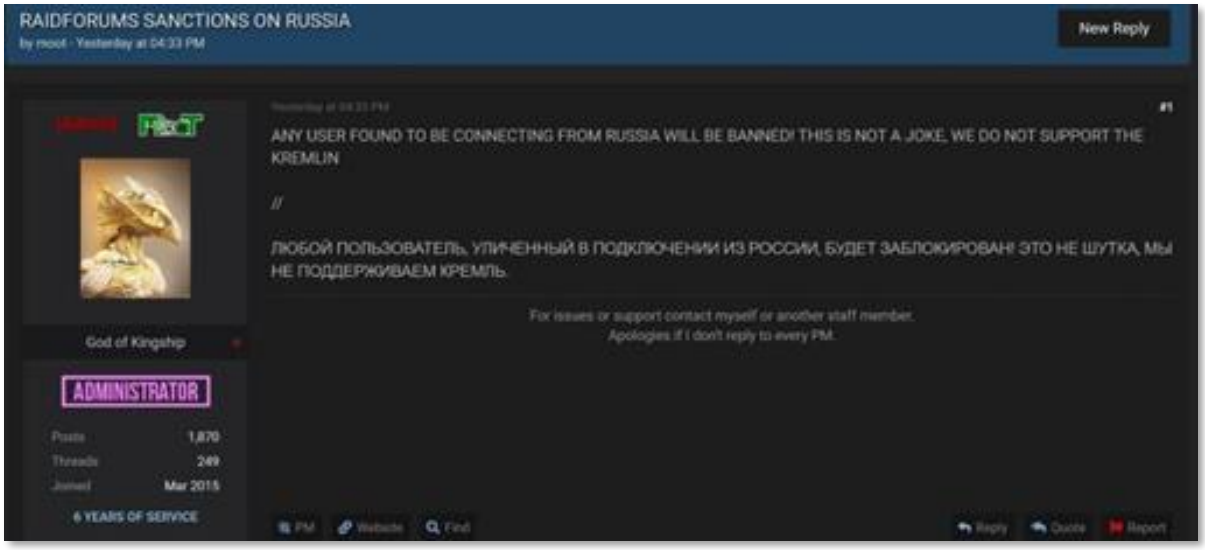


Figure 2: Raidforum admin "MOOT"'s posting regarding the implemented anti-Russia stance

As of publication at least two (2) successor websites have been created in the wake of this Raidforums takedown. The first site is "Breached[.]co," also known as "BreachedForum." As of the end of March 2022, BreachedForum has accumulated approximately 1,499 registered users in under one (1) month. Former Raidforums admin "pompompurin" appears to have been the individual behind this new website,[11] intending for it to become the legitimate Raidforums successor rather than allow other forums to capitalize on the vacuum created by Raidforums' absence.

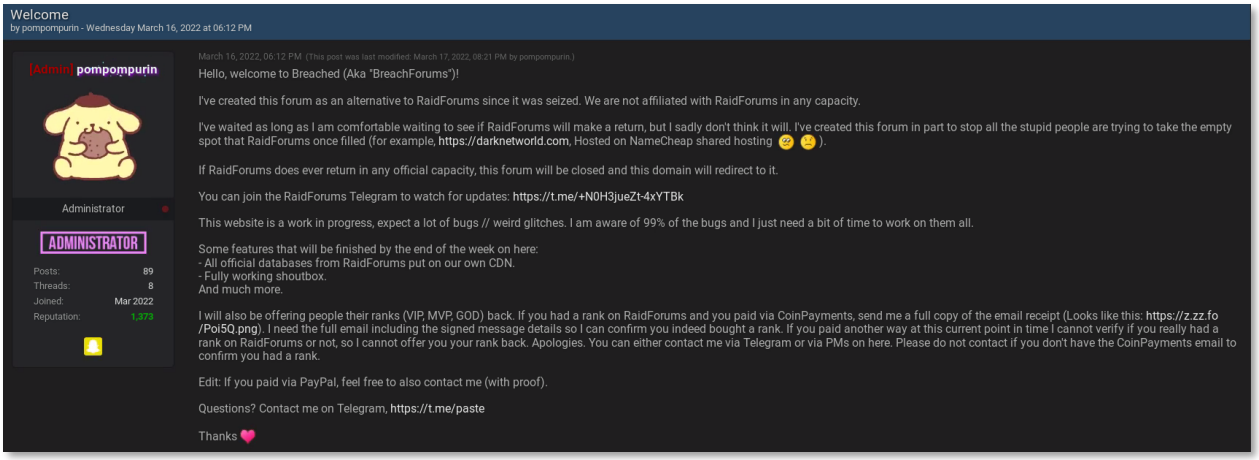


Figure 3: BreachedForum admin "pompompurin"'s welcome posting

The user interface (UI) of BreachedForum is nearly identical to that of Raidforums. New features to fully recreate the original setup are constantly being added with "pompompurin" appearing to be working consistently on updates for the website. This website appears to be hosting an active community with consistent posts across multiple forum categories with various discussions and leaks being present. It is apparent that BreachedForum administrators have set themselves up for success, and the website appears to be the most popular direct successor to Raidforums thus far.

[11] https://www.databreaches.net/while-questions-about-raidforums-remain-unanswered-breachforums-opens/

The second attempted successor to Raidforums has been “raidforums2[.]com” (also known as “Raid2”). This instance appears to have been created by a pro-Ukrainian group previously present on Raidforums who focused on working with the all-volunteer “Ukraine IT Army” to coordinate attacks against Russian assets. Raid2 has not experienced the same level of success as BreachedForum as it is currently hosting 814 registered members as of this publication. Admin “Burkeluke” appears to oversee Raid2 and has been observed making general announcements regarding the website. “Burkeluke” has also posted multiple leaks from various Russian agencies as well as additional Russian assets in recent weeks. Raid2 has had a slower growth rate and less activity than BreachedForum, but it appears to still have a consistent user base and some coordination with other factions to continue anti-Russian/pro-Ukrainian activities along with various other side leaks.

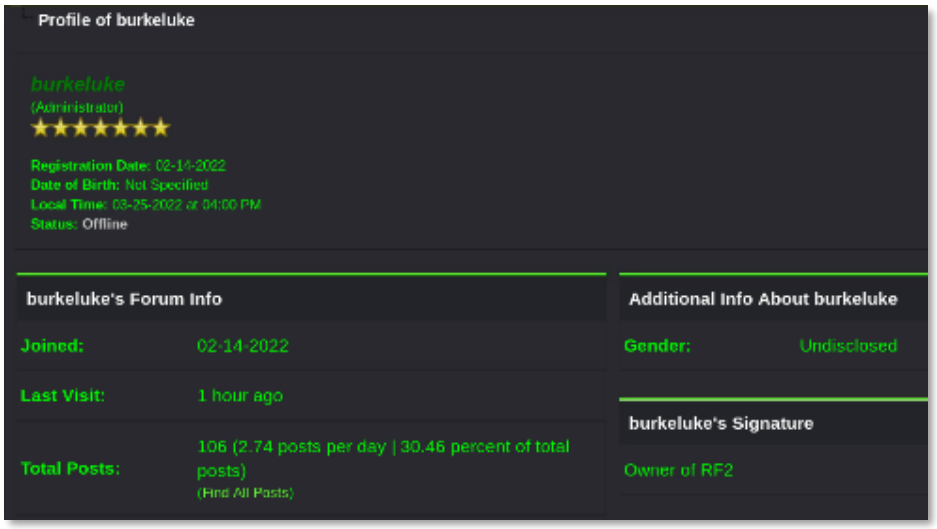


Figure 4: Profile of Raid2 admin “Burkeluke”

Raidforums users have also appeared to migrate to other well-known and previously established forums. According to “Webz[.]io,” websites such as “Crackx,” “Dread,” and “wwh-club” observed sharp spikes in new users in the ten (10) days following the Raidforums seizure.[12] Russian sites such as “XSS”, and “wwh-club”, are speculated to be the now-favored sites of many Russian users of Raidforums due to Raidforums’ stance on Russia as well as the possibility that BreachedForum could maintain anti-Russian posturing, similar to Raid2. CTIX analysts will continue to monitor the unknown aspects of Raidforums’ seizure, the successor websites that have filled the void, and how the influx of new users to various forums impacts the overall forum environment.

[12] https://webz.io/dwp/raidforum-is-seized-where-will-its-users-go-now/

APT41 TARGETING UNITED STATES STATE GOVERNMENT ENTITIES

Key Points

- Chinese-backed nation-state threat group APT41 successfully compromised at least six (6) US state government networks by exploiting the Log4j flaw as well as a USAHerds application vulnerability.
- In 2020, APT41 was very active, and utilized various vulnerabilities, such as Citrix NetScaler Application Delivery Controller (ADC), Zoho ManageEngine, and Cisco RV320 routers to target an array of industries globally in order to fulfill their financially driven motives.
- Although APT41 is historically known for actively scanning for known exploitable vulnerabilities, it is likely that this utilization of Log4j may have simply been a target of opportunity. It is common knowledge by threat actors that many organizations have yet to patch their vulnerable systems.

Summary

Advanced Persistent Threat 41 (APT41), a known sophisticated threat organization, has been targeting United States state government entities and gaining access to their infrastructure. APT41 is Chinese-backed nation-state threat operation that has been active since 2012 and is a key part of the Winnti Umbrella Group, a cluster of similar Chinese threat groups conducting cybercrime operations. Threat actors from APT41 are highly motivated with the end goal of exploiting targets for cyber espionage purposes in order to benefit the Chinese state. In addition to espionage, APT41 actors are extremely financially driven and primarily focus on the gaming and cryptocurrency industries to fulfill these operations. Historically, APT41's cyber espionage operations have targeted countries worldwide, including the United States, United Kingdom, Switzerland, France, India, Italy, Japan, Myanmar, the Netherlands, and more.

In 2020, the group was linked to a large-scale espionage operation that targeted vulnerabilities within the Citrix NetScaler Application Delivery Controller (ADC) in addition to Zoho ManageEngine and Cisco RV320 routers. This operation targeted over seventy (70) global organizations within nineteen (19) different industries, including the financial, construction, healthcare, advanced technology, telecommunications, pharmaceutical, transportation, government, and defense sectors. The operation lasted approximately two (2) months and is considered one of the major cyber-espionage campaigns carried out by Chinese state hackers.

Within roughly the last year, activity from the APT41 threat group has continued to rise. Specifically, threat actors compromised six (6) United States state government entities, in all cases where the point-of-compromise was a device vulnerable to the Log4j flaw (tracked as CVE-2021-44228). In addition to Log4j, APT41 actors also utilized another unsuspected vulnerability that targets the USAHerds application (CVE-2021-44207) which is primarily utilized for agricultural and livestock management issues. In one such case of state government compromise, APT41 actors breached the integrity of the victim network and deployed a new variant of the "KeyPlug" backdoor. KeyPlug targets Linux systems to establish a secure connection to actor-controlled command-and-control (C2) nodes utilizing several networking protocols. In other compromises from the organization, actors would further deploy shells and scripts onto victim's devices for data exfiltration, credential harvesting, espionage, and masking the attacks with anti-analysis techniques to evade security analysts. In early March of 2022, cybersecurity firm Mandiant released a comprehensive report detailing that a Chinese state hacking group was observed exploiting the infamous Log4Shell vulnerability.[13] They claimed the activity was monitored between May 2021 and February 2022, and was

[13] https://www.mandiant.com/resources/apt41-us-state-governments

indicative of a deliberate cyber espionage campaign.[14] Although researchers from Mandiant did attribute the activity to APT41, they could not definitively gauge if the threat actor was operating on behalf of the Chinese state, or conducting attacks for their own personal gain.

[14] https://www.mandiant.com/resources/apt41-us-state-governments

THREAT ACTOR OF THE MONTH

Key Points

- Lapsus$ is an extremely active yet inexperienced extortion group.
- The group has targeted various large companies, such as Nvidia, Samsung, Microsoft, and Okta.
- Members of Lapsus$ have recently been in the spotlight for their arrests as well as being doxed by adversaries.

Summary

Lapsus$, a relatively new but extremely prolific hacking group operating globally, has seen some law enforcement action recently but shows no signs of slowing down. Little is known about the group, but it is believed to be based in South America with global members and is comprised of teenagers and young adults. While Lapsus$ is often grouped into the ransomware category, the threat group does not generally encrypt the machines that they attack. Since February 2022, Lapsus$ has claimed responsibility for:

- Nvidia: Lapsus$ claimed that they stole one (1) terabyte (TB) of internal data from the company including employee credentials, documentation, private tools, SDKs, as well as information about their proprietary drivers, schematics, and firmware.[15] A Lapsus$ member recently tried to extort Nvidia for $10 million; this, however, was an unreasonable ransom amount to demand. The Lapsus$ leadership understood this themselves and publicly outed which member was responsible afterwards.

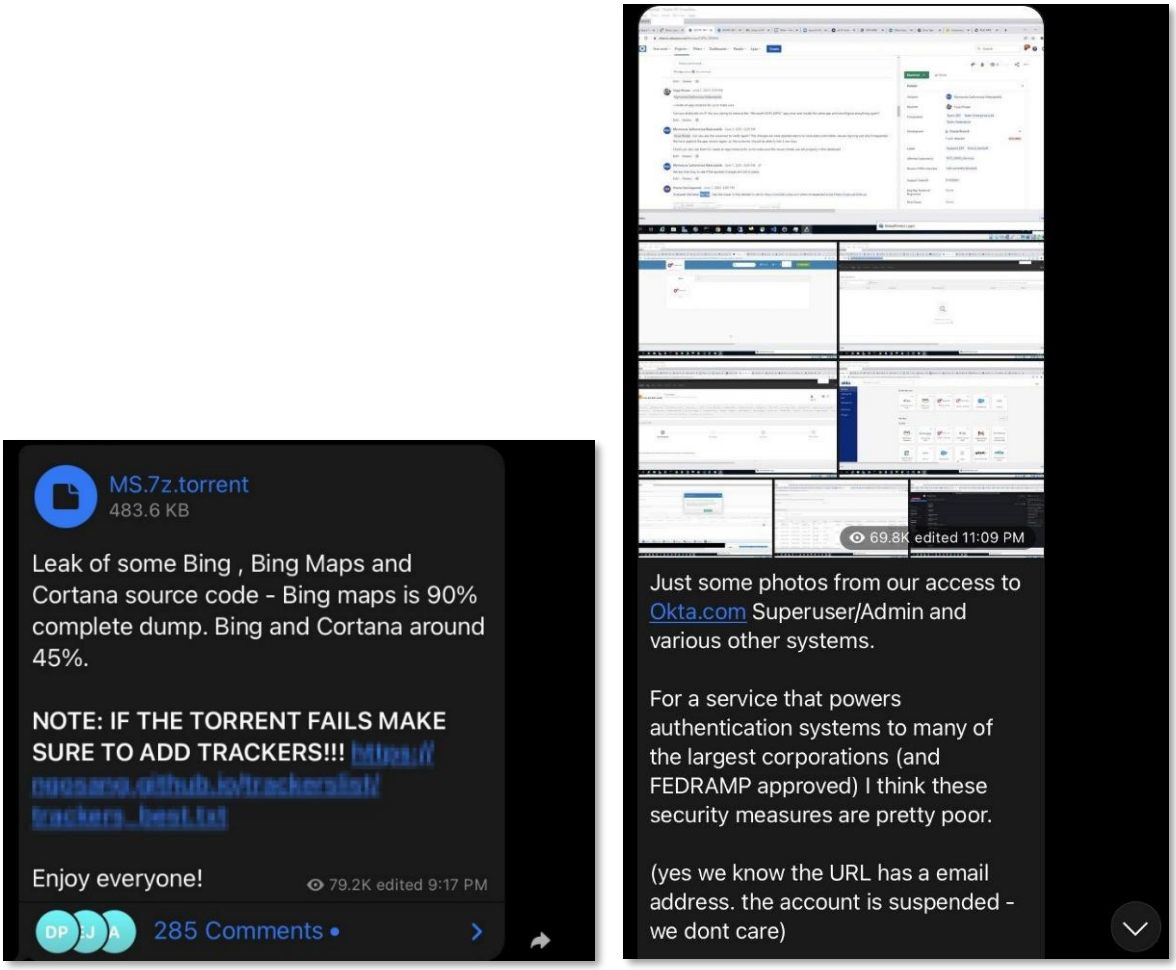
- Microsoft: In the Microsoft breach, Lapsus$ leaked screenshots of the Microsoft internal devops instance and claimed to have access to the source code for Bing and Cortana.[16] The threat group stated that they leaked about 90% of Bing's maps along with 45% of Bing and Cortana's source code.

- Samsung: Lapsus$ leaked approximately 190 gigabytes (GBs) of archives containing confidential data that they claimed was from Samsung.[17] Samsung did confirm that its network was breached, and that sensitive information was exfiltrated by undisclosed actors.[18] In a statement to Bloomberg, Samsung detailed that "the breach involves some source code relating to the operation of Galaxy devices but does not include the personal information of our customers or employees".[19]

- Okta: In late March of 2022, Lapsus$ targeted Okta, a multi-factor authentication and access management platform. Investigators discovered Lapsus$ gained access to a third-party provider Sitel which gave them access to 366 companies through their Okta accounts.[20] In the screenshots that Lapsus$ leaked regarding Okta, the group displayed images of the administrator account name of which they accessed and utilized to access hundreds of Okta tenants from many different companies. This reveal provides insight into how inexperienced the group currently is.

---

[15] https://www.bleepingcomputer.com/news/security/nvidia-data-breach-exposed-credentials-of-over-71-000-employees/
[16] https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-they-were-hacked-by-lapsus-extortion-group/
[17] https://www.bleepingcomputer.com/news/security/samsung-confirms-hackers-stole-galaxy-devices-source-code/
[18] https://www.bleepingcomputer.com/news/security/samsung-confirms-hackers-stole-galaxy-devices-source-code/
[19] https://www.bloomberg.com/news/articles/2022-03-07/samsung-says-hackers-breached-company-data-galaxy-source-code
[20] https://therecord.media/okta-revises-original-statement-says-hundreds-of-customers-affected-by-lapsus-breach/



Figures 5 and 6: Lapsus$'s Telegram posts regarding Bing, Cortana, and Okta

A member of Lapsus$, who goes by the handles “White” and “Breachbase”, was doxed in early January by a prolific doxer who goes by the name “Vile” on a dox site owned by “KT”. According to the information leaked in the dox, there is some history between “White” and “KT.” “KT” previously owned the prolific dox site “doxbin,” which he then sold to “White” only to buy it back after it began to fail. This dox involved sensitive, personal information including his name, home addresses, leaked conversations, pictures of his house, all of his known aliases, and more.

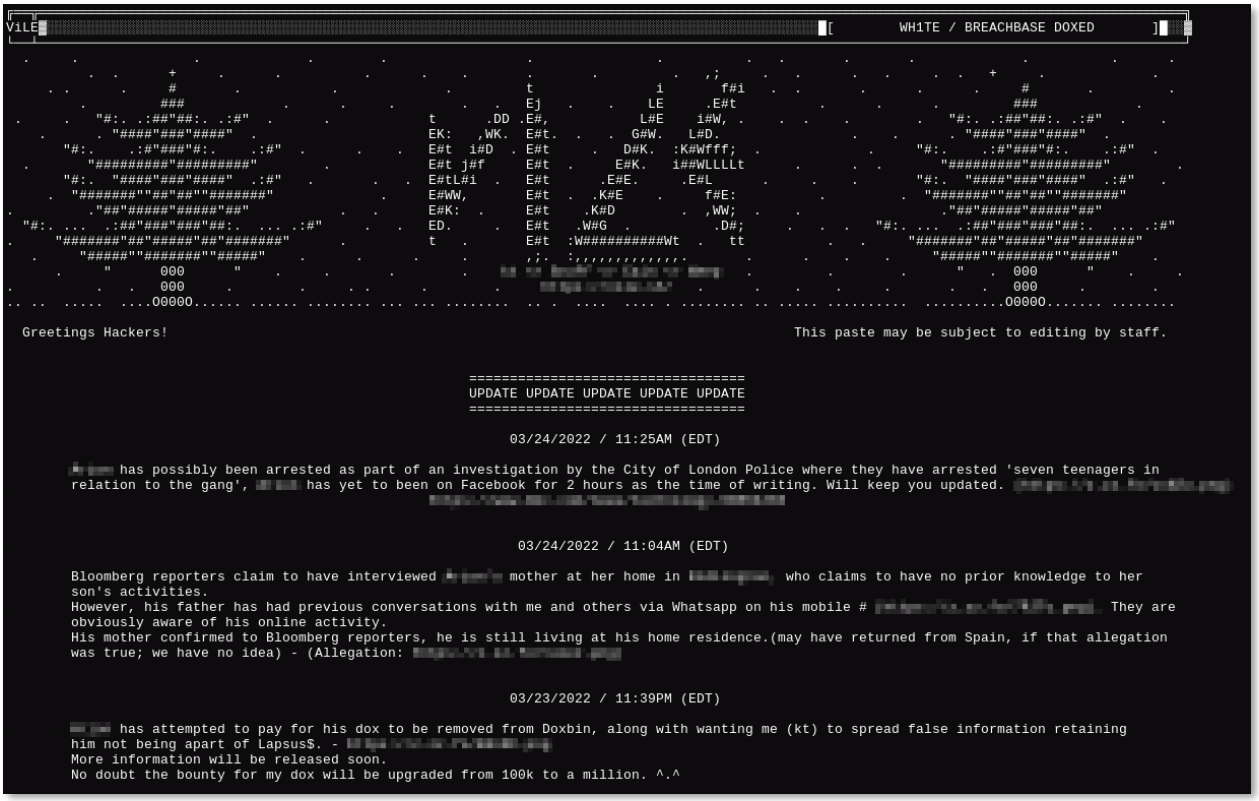


Figure 7: "Vile"'s dox about "White"

Following the doxing of "White," City of London police arrested seven (7) individuals associated with the Lapsus$ group on March 31st, 2022. All of the arrested individuals ranged from the ages of sixteen (16) to twenty-one (21), one of whom was identified to be the user "White." On April 2nd, 2022, two (2) of the seven (7) individuals were charged with "three counts of unauthorised access with intent to impair operation of, or hinder, access to a computer, and two counts of fraud by false representation."[21] One (1) of the two (2) individuals was also charged with "one count of causing a computer to perform a function to secure unauthorised access to a programme."[22] Due to legal restrictions, the names of the two individuals, aged sixteen (16) and seventeen (17), remain undisclosed.

Just one (1) day before the arrests, Lapsus$ stated that some of their members were on a "vacation," and would return on the 30th of March. Upon their return from vacation, Lapsus$ leaked seventy (70) GBs of data from Globant, an IT and software development company.[23] Globant confirmed this data leak and stated that the data consisted of "certain source code and project-related documentation for a very limited number of clients."[24] Lapsus$ provided a screenshot of a selection of source code folders that were accessed, including "Abbott, apple-heath-app, C-span, Fortune, Facebook, DHL, and Arcserve."[25] The fallout from the exfiltration of this sensitive data is still being quantified.

Despite the Lapsus$ group being made up of teenagers and young adults, they have proven that they can breach some of the largest companies worldwide in a quick manner. However, their lack of experience is

[21] https://www.bbc.com/news/technology-60953527
[22] https://www.bbc.com/news/technology-60953527
[23] https://www.bleepingcomputer.com/news/security/globant-confirms-hack-after-lapsus-leaks-70gb-of-stolen-data/
[24] https://www.globant.com/news/globant-official-update
[25] https://www.bleepingcomputer.com/news/security/globant-confirms-hack-after-lapsus-leaks-70gb-of-stolen-data/

beginning to catch up with them and CTIX analysts do not expect it to be the last time showcasing this characteristic. Due to the chaotic unpredictability of the Lapsus$ gang's next steps, security analysts must continue to actively monitor their tactics, techniques, and procedures. CTIX analysts predict that Lapsus$ will continue their operations despite the publicity surrounding the group in order to remain in the spotlight.

Trending IOCs

The following technical indicators of compromise (IOCs) are associated with monitored threat groups and/or campaigns of interest within the past sixty (60) days. IOCs can be utilized by organizations to detect security incidents more quickly and easily, as indicators may not have otherwise been flagged as suspicious or malicious.

Indicator	Type	Attribution
ipfltdrvs.sys	File Name	Daxin Backdoor
ndislan.sys	File Name	Daxin Backdoor
ndislan_win2008_x64.sys	File Name	Daxin Backdoor
81c7bb39100d358f8286da5e9aa838606c98dfcc263e9a82ed91cd438cb130d1	Hash-256	Backdoor.Daxin (32-bit core)
06a0ec9a316eb89cb041b1907918e3ad3b03842ec65f004f6fa74d57955573a4	Hash-256	Backdoor.Daxin (64-bit core)
7a7e8df7173387aec593e4fe2b45520ea3156c5f810d2bb1b2784efd1c922376	Hash-256	Daxin Backdoor - Backdoor.Zala (32-bit core)
8dafe5f3d0527b66f6857559e3c81872699003e0f2ffda9202a1b5e29db2002e	Hash-256	Daxin Backdoor - Backdoor.Zala (32-bit core)
514d389ce87481fe1fc6549a090acf0da013b897e282ff2ef26f783bd5355a01	Hash-256	Daxin Backdoor - Trojan.Emulov (core)
1a5c23a7736b60c14dc50bf9e802db3fcd5b6c93682bc40141d6794ae96138d3	Hash-256	Daxin Backdoor - Trojan.Emulov (dropper)
a0ac5f7d41e9801b531f8ca333c31021c5e064f13699dbd72f3dfd429f19bb26	Hash-256	Daxin Backdoor - Trojan.Owprox (core)
aa7047a3017190c66568814eb70483bf74c1163fb4ec1c515c1de29df18e26d7	Hash-256	Daxin Backdoor - Trojan.Owprox (dropper)