UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORPORATION, a Washington Corporation, FORTRA, LLC, a Delaware Limited Liability Company, and HEALTH-ISAC, INC., a Florida Corporation,

Plaintiff,

v.

JOHN DOES 1-2, JOHN DOES 3-4 (AKA CONTI RANSOMWARE GROUP), JOHN DOES 5-6 (AKA LOCKBIT RANSOMWARE GROUP), JOHN DOES 7-8 (AKA DEV-0193), JOHN DOES 9-10 (AKA DEV-0206), JOHN DOES 11-12 (AKA DEV-0237), JOHN DOES 13-14 (AKA DEV-0243), JOHN DOES 15-16 (AKA DEV-0504), Controlling Computer Networks and Thereby Injuring Plaintiffs and Their Customers,

Defendants.

Case No.

FILED UNDER SEAL

DECLARATION OF JASON B. LYONS IN SUPPORT OF APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Jason B. Lyons, declare as follows:

1. I am a Principal Manager of Investigations in Microsoft Corporation's Digital Crimes Unit ("DCU") Ransomware Team. I make this declaration in support of Microsoft's Application for An Emergency Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where indicated. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. In my role at Microsoft, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business and customers. Among my responsibilities are protecting Microsoft's online service assets from network-based attacks. I also participate in the investigation of malware and participate in court-authorized countermeasures to neutralize and disrupt malware. For example, I have personally investigated and assisted in the court-authorized takedown of several families of malware or botnets while at Microsoft, including the malware families and botnets known as Ramnit, ZeroAccess, Dorkbot, and Necurs. Before joining Microsoft, I worked for Xerox as the Manager of Xerox's Cyber Intelligence Response Team. I also worked for Affiliated Computer Services ("ACS") prior to Xerox's acquisition of ACS. While at ACS, I provided in-court testimony in connection with a temporary restraining order application concerning misappropriation of ACS's intellectual property. Prior to entering the private sector, from 1998 to 2005, I served as a Counterintelligence Special Agent in the United States Army. My duties as a Counterintelligence Special Agent included investigating and combating cyber-attacks against the United States. I obtained certifications in counterintelligence, digital forensics, computer crime investigations, and digital media collection from the United States Department of Defense. A true and correct copy of the current version of my curricula vitae is attached to this declaration as **Exhibit 1**.

3. I have investigated the structure and function of Cobalt Strike[1] as well as the

[1] Cobalt Strike is a post exploitation tool that is a threat emulation product offered by Plaintiff

activities carried out through the use of cracked versions of Cobalt Strike[2], and an assessment of the impact on Microsoft's business and on users of the Internet. Misuse of Cobalt Strike has caused, and continues to cause, extreme damage to Microsoft and other parties, which if allowed to continue, will be compounded as the case proceeds.

I. DEFENDANTS

4. The identities and specific locations of the Defendants who have set up and currently misuse cracked versions Cobalt Strike to carry out ransomware attacks are currently uncertain. However, we have detected many instances of the malicious use of Cobalt Strike and Cobalt Strike command and control ("C2") infrastructure in many different countries, including the United States, and it is probable that the criminals operating the C2 infrastructure are also located in different countries. Specifically, we have identified Cobalt Strike C2 infrastructure and affected victims as being located in the State of New York, particularly in cities and counties within the Eastern District of New York. *See* ¶ 23 *infra*; *see also* Coy Decl. ¶¶ 38-39.

5. Defendants control Cobalt Strike through C2 infrastructure comprised of IP addresses and domains maintained on an interconnected network. They use common tools, a common codebase, and common tactics to establish and run malware and ransomware, and they appear to share C2 resources. The Defendants use the Cobalt Strike C2 infrastructure to carry out ransomware and malware attacks and related criminal activity.

II. THE INVESTIGATION OF COBALT STRIKE

6. Cobalt Strike is a commercial penetration testing tool that has been used by threat

---

Fortra LLC which is used to conduct penetration testing. As offered, Cobalt Strike is a legitimate commercial penetration testing framework that has been notoriously abused by threat actors to carry out ransomware acts. The Declaration of Christopher Coy filed concurrently with Plaintiffs' Application for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction ("Coy Decl.") describes the functionality of Cobalt Strike. *See* Coy Decl. at ¶¶ 4, 7-8; *see also* Declaration of Robert Erdman filed concurrently with Plaintiffs' Application for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction ¶¶ 6-7.

[2] As used in this declaration and in others, "cracked versions of Cobalt Strike" refer to stolen, unlicensed, or otherwise unauthorized versions or copies of Cobalt Strike.

actors for the purpose of delivering ransomware and malware to infect victim computers. As described in the Coy Declaration, at issue here are the "cracked" versions of Cobalt Strike, which are defined as "[c]ompromised versions of Cobalt Strike" and "often consist of manipulated beacon files that are programmed to communicate with the malicious command and control infrastructure to engage in illegal activities once a malware infiltrates a victim's systems." *See* Coy Decl. at ¶ 9. Microsoft investigators and I have been able to identify operational details about cracked versions of Cobalt Strike, including its C2 infrastructure, the methods of communication among infected computers, how Cobalt Strike is used to transmit threats to innocent computers, and the criminal enterprise's mechanisms to evade detection and attempts to disrupt its operation. Cracked versions of Cobalt Strike are used to infect approximately 1.5 million unique computing devices around the world in the past twenty-four months alone. While Cobalt Strike is a legitimate commercial product, cracked and misused versions of Cobalt Strike can be utilized as providing backdoor access to infected machines and acting as a gateway malware dropper to deploy additional ransomware. As I describe in this declaration, once deployed, Cobalt Strike can be used to deliver the following ransomware families to the victims' machine: Conti, LockBit, Quantum Locker, Royal, Cuba, BlackBasta BlackCat, and PlayCrypt.

7. I have obtained copies of cracked Cobalt Strike, and I have examined them. I have researched the C2 infrastructure that is used to propagate Cobalt Strike. I have also reviewed literature published by other well-regarded computer security investigators concerning Cobalt Strike, and their findings have confirmed my own conclusions regarding Cobalt Strike and the misuse of Cobalt Strike to deliver ransomware. Through these and related investigative steps, I have developed detailed information about the size, scope, and illegal activities of cracked versions of Cobalt Strike.

8. In the course of Microsoft's investigation into Cobalt Strike, we analyzed approximately 50,000 unique samples of cracked Cobalt Strike. Microsoft investigators and I purposely deployed cracked versions of Cobalt Strike to investigator-controlled computers, and we observed cracked Cobalt Strike C2 infrastructure, in order to understand its operation. This

allowed us to monitor and analyze the Cobalt Strike infrastructure in order to understand its lifecycle. I participated in and reviewed these investigative techniques.

9. During our investigation, Microsoft investigators and I observed the infected computers that connect to and receive instructions from C2 servers associated with cracked versions of Cobalt Strike; and through this method, we were able to identify IP addresses and domains of the C2 servers used to control cracked versions of Cobalt Strike. Based on my examination of aforementioned identified IP addresses and domains, I was able to ascertain particular technical features and behaviors associated with those IP addresses and domains, which further allowed me to confirm that new IP addresses and domains are associated with cracked versions of Cobalt Strike. This verification process has enabled me to accurately identify C2 servers associated with cracked versions of Cobalt Strike that should be disabled.

10. Based on our investigation and analysis, Microsoft has determined that cracked versions of Cobalt Strike are a substantial and robust delivery mechanism for distributing ransomware such as Conti, LockBit, Quantum Locker, Royal, Cuba, BlackBasta BlackCat, and PlayCrypt. Further detailed description regarding the Conti and LockBit ransomware is set forth below at ¶¶ 28-33.

III. IDENTIFICATION OF CRACKED VERSIONS OF COBALT STRIKE

11. Because Cobalt Strike is a legitimate commercial product, I was responsible for investigating and identifying the cracked versions of Cobalt Strike which have been used by threat actors and comprise part of the Cobalt Strike C2 infrastructure. I have evaluated the watermarks associated with Cobalt Strike licenses and deployed a crawler to identify cracked versions of Cobalt Strike. Both processes are described herein.

A. Cobalt Strike Watermarks

12. Each legitimate Cobalt Strike license contains a unique watermark—a unique value associated with a specific Cobalt Strike license. Cobalt Strike watermarks can be identified in post incident analysis and are considered valued intelligence in the security community.

13. Where a version of Cobalt Strike is cracked, any value can be placed in the watermark file, such that many versions of Cobalt Strike will have the same, illegitimate watermark. *See* Coy Decl. ¶ 8, n.3. Through post incident analysis, we have been able to associate certain watermarks with various threat actor groups. For example, in analyzing approximately 50,000 unique samples, I have observed the following exemplary watermarks as being associated with cracked versions of Cobalt Strike: 666, 1234567890. These are only examples, and the figure below describes other observed watermarks that have been associated with specific threat groups or ransomware families:

14. For example, the watermark "1580103824" has been associated with the "Elbrus" activity group, which is linked to financially-related ransomware attacks. As described in the declaration of Errol Weiss, the Chief Security Officer of Plaintiff H-ISAC ("Weiss Decl."), healthcare institutions have been harmed by these attacks, and these attacks are carried out through the use of cracked versions of Cobalt Strike. Weiss Decl. ¶¶ 14-15. As another example, in May 2021, Ireland's Health Service Executive was subjected to a serious criminal cyberattack using Conti ransomware. It is believed that a cracked version of Cobalt Strike was used to carry out the cyberattack. *See* PricewaterhouseCoopers, *Conti cyber attack on the HSE: Independent Post Incident Review*, Report (Dec. 03, 2021).[3]

B. Deployment of Crawler for Purposes of Identifying Cracked Cobalt Strike

15. Microsoft Defender is the anti-malware component of Microsoft Windows, which is built into the Windows operating system. Currently, Microsoft Defender is capable of detecting Cobalt Strike as malware, as are several other anti-virus programs. However, end-users who have not enabled Defender or other antivirus software are at risk of compromise by cracked versions of Cobalt Strike, and other malware which can be delivered through those cracked versions. As part of Defender's operation, the software will collect the Cobalt Strike configuration files (also known

[3] Available at https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

as a "beacon file"). These configuration files comprise one of the data sources used in connection with the "crawler" used to identify and confirm cracked Cobalt Strike C2 infrastructure. The figure below depicts an example configuration file.

```
{
    "Config": {
        "BeaconType": "HTTP",
        "Port": 80,
        "SleepTime": 45000,
        "MaxGetSize": 1403644,
        "Jitter": 37,
        "PublicKey": "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC3g7RiGbQy+cNxbjWG1xpYkAw1c29/<REDUCTED>AAA==",
        "C2Server": "dns.adspay.io,/jquary-3.3.1.min.js",
        "SpawnTo": "AAAAAAAAAAAAAAAAAAAAAA==",
        "Spawnto_x86": "%windir%\\syswow64\\dllhost.exe",
        "Spawnto_x64": "%windir%\\sysnative\\dllhost.exe",
        "CryptoScheme": 0,
        "HttpGet_Verb": "GET",
        "HttpPost_Verb": "POST",
        "HttpPostChunk": 0,
        "Watermark": 100000,
        "bStageCleanup": "True",
        "bCFGCaution": "False",
        "UserAgent": "Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko",
        "HttpPostUri": "/jquary-3.3.2.min.js",
        "HttpGet_Metadata": "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8,Referer: http://code.jquery.com/,Accept-Encoding: gzip, deflate,__cfduid=,Cookie",
        "HttpPost_Metadata": "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8,Referer: http://code.jquery.com/,Accept-Encoding: gzip, deflate,__cfduid",
        "HostHeader": "",
        "bUsesCookies": "True",
        "Proxy_Behavior": "Use IE settings",
        "KillDate": null,
        "bProcInject_StartRWX": "False",
        "bProcInject_UseRWX": "False",
        "bProcInject_MinAllocSize": 17500,
        "ProcInject_PrependAppend_x86": "kJA=,Empty",
        "ProcInject_PrependAppend_x64": "kJA=,Empty",
        "ProcInject_Execute": "CreateThread_",
        "ProcInject_AllocationMethod": "NtMapViewOfSection"
    }
}
```


FIGURE 1 – Cracked Cobalt Strike Configuration File

16. As shown in the figure, the configuration file contains information that allows me to identify the corresponding watermark for a particular configuration file. This allows me to determine if the version of Cobalt Strike that is associated with specified configuration file is an cracked version. This figure also shows the IP address associated with each version of Cobalt Strike. Where the configuration file demonstrates that the associated version of Cobalt Strike is cracked or being used by threat actors, the IP address or domain allows Microsoft to identify the C2 infrastructure that Plaintiffs are requesting be taken down or access blocked in connection with their TRO and Preliminary Injunction. Exhibit 2 to the Coy Declaration (Appendix A to the Complaint) identifies the IP addresses and domains that are subject to Plaintiffs' takedown request.

17. Additionally, the DCU and I use and rely on other data sources in connection with the crawler. For example, Shodan is an external intelligence provider that we use for data and

information collection in the DCU. Shodan scans the internet to collect publicly available information about various devices that are connected to the internet—if a device is directly hooked up to the Internet, then Shodan is able to query it for publicly-available information.[4] Shodan also collects Cobalt Strike configuration files via its own crawler. The DCU investigators and I obtain and use the Shodan intelligence in connection with our own crawler. Similarly, DCU also obtains information for use with its crawler from Microsoft Defender Threat Intelligence Team (previously known as Risk IQ, another cyber security company, before acquisition by Microsoft). Many threat intelligence companies sell Cobalt Strike C2 data as a threat intelligence product so that their customers can further protect themselves against nefarious uses of Cobalt Strike.

18. These configuration files, both those collected from Windows Defender and collected from external sources, are the main input for the DCU crawler. The purpose of crawling is to track the cracked Cobalt Strike infrastructure. The purpose of crawling the cracked Cobalt Strike infrastructure is to have a high-fidelity signal that the infrastructure is active and being used by threat actors. The diagram below illustrates the steps the crawler takes that allow me to identify cracked Cobalt Strike C2 infrastructure.

19. The below figure depicts the crawler methodology used to identify cracked Cobalt Strike C2 infrastructure:

---

[4] *See* "What is Shodan?" *Shodan Help Center*, (last visited Mar. 12, 2023), available at https://help.shodan.io/the-basics/what-is-shodan ("Shodan is a search engine for Internet-connected devices. Web search engines, such as Google and Bing, are great for finding websites. But what if you're interested in measuring which countries are becoming more connected? Or if you want to know which version of Microsoft IIS is the most popular? Or you want to find the control servers for malware? Maybe a new vulnerability came out and you want to see how many hosts it could affect? Traditional web search engines don't let you answer those questions. Shodan gathers information about all devices directly connected to the Internet. If a device is directly hooked up to the Internet then Shodan queries it for various publicly-available information. The types of devices that are indexed can vary tremendously: ranging from small desktops up to nuclear power plants and everything in between. So what does Shodan index then? The bulk of the data is taken from banners, which are metadata about a software that's running on a device. This can be information about the server software, what options the service supports, a welcome message or anything else that the client would like to know before interacting with the server.").

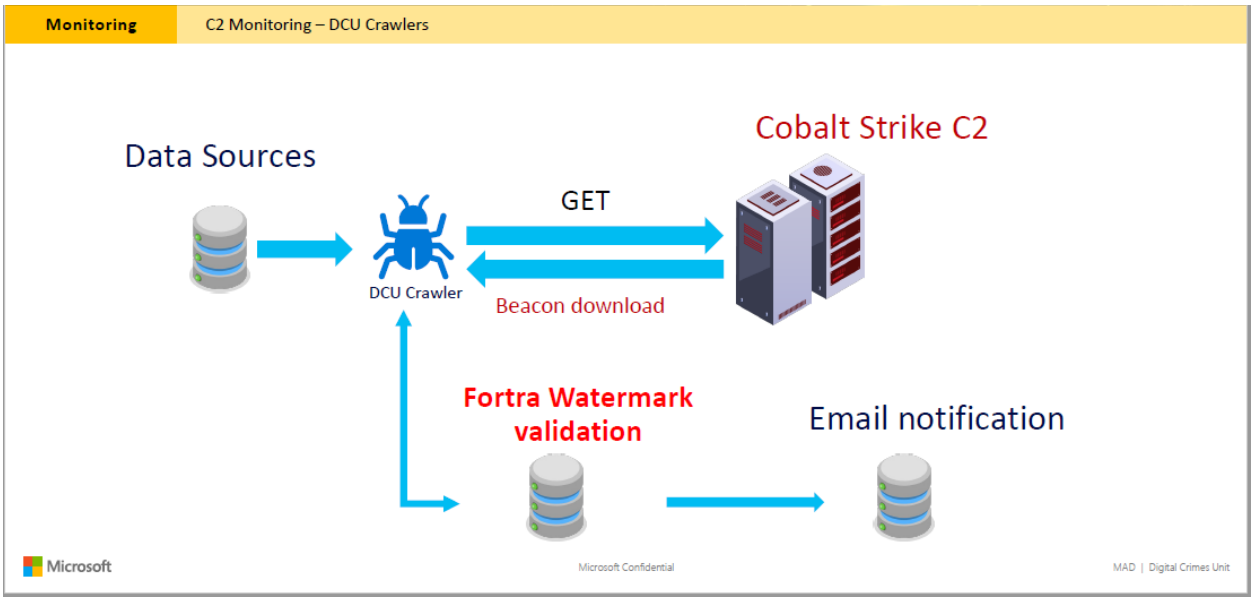


FIGURE 2 – Crawler Methodology

20. To determine whether the Cobalt Strike C2 infrastructure is delivering a malicious payload, first the crawler receives input from a data source, such as an IP address or domain. Next, using this input, the crawler communicates with the Cobalt Strike C2 infrastructure using the "GET" command. In the above Figure 2 (illustrating the configuration file), the GET command sequence is notated with a red box. Once the crawler communicates with the Cobalt Strike C2 infrastructure, it downloads the beacon payload (or configuration file) with the associated universal resource identifier ("URI"). After the download, the payload data is extracted and the watermark value for a specific configuration file is compared to the known malicious watermarks. If the watermark matches a known malicious watermark, that instance of Cobalt Strike is determined to be cracked or maliciously used. As part of the investigation, DCU receives telemetry from Fortra regarding their watermark assessment and validation, which I understand to be their internal processes designed to identify and validate watermarks associated with cracked Cobalt Strike. In connection with our investigation, we rely on the watermark validation that Fortra has provided. Fortra's watermark validation informs the rest of the DCU and my analysis. Based on my experience and the information that is available to the DCU, I have no reason to doubt the accuracy

of the Fortra watermark validation data.

21. Once a successful download of a beacon file has occurred (successful being defined as the identification of a malicious instance of Cobalt Strike), the geolocation of the IP address and ASN (autonomous system is a collection of connected IP routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain) information is collected. At DCU, we track the geolocation of malicious Cobalt Strike to ascertain the locations where the malicious activity is more prominent. The below figures depict geolocation of malicious Cobalt Strike infrastructure for the United States and in the Eastern District of New York. The figures depict locations where a high quantity of malicious Cobalt Strike C2 infrastructure is located within the United States and the Eastern District of New York. As depicted in the following heatmaps, the darker color represents geographic areas with more infections, while the circle size demonstrates the geographic range of the infection.

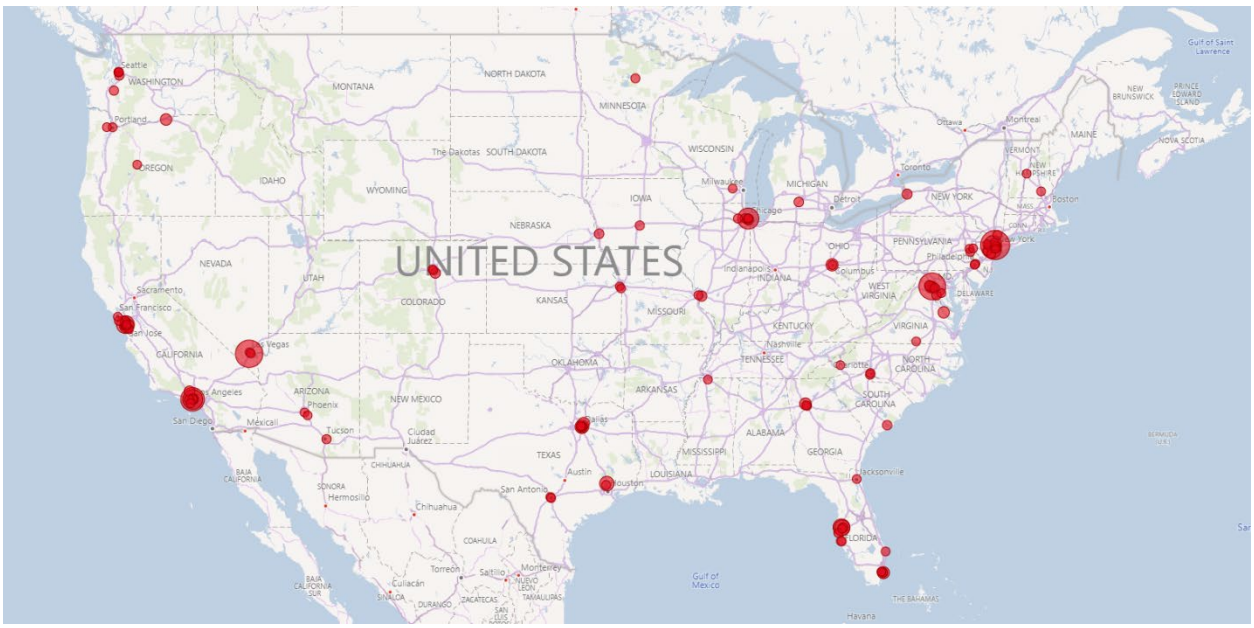


FIGURE 3 – Cracked Cobalt Strike C2 Infrastructure (US)

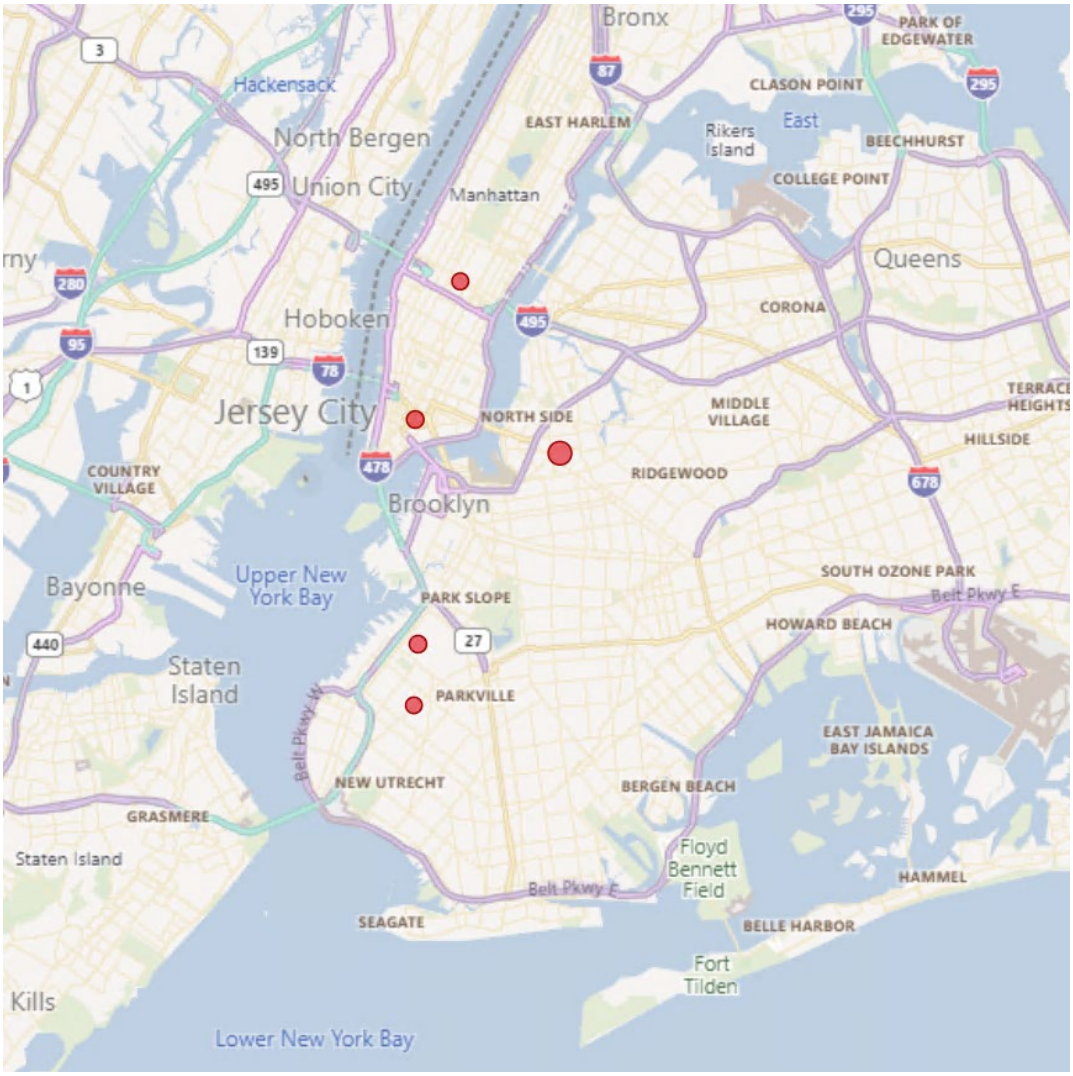


FIGURE 4 – Cracked Cobalt Strike C2 Infrastructure (Eastern District of New York)

22. This information allows us to ascertain the IP addresses and domains that have been used to deliver cracked Cobalt Strike. A full list of the IP addresses and domains are included as Exhibit 2 to the Coy Declaration (Appendix A to the Complaint).

23. Using information from the crawler as well as information from Defender, we are able to identify the victims of malicious Cobalt Strike. The figure below depicts the geolocation of victim locations, which represents approximately 1.5 million infected unique machines in a twenty-four month period predating the filing of this action. As shown in the figure, there are large numbers of such victims located throughout the United States and in the Eastern District of New

York.

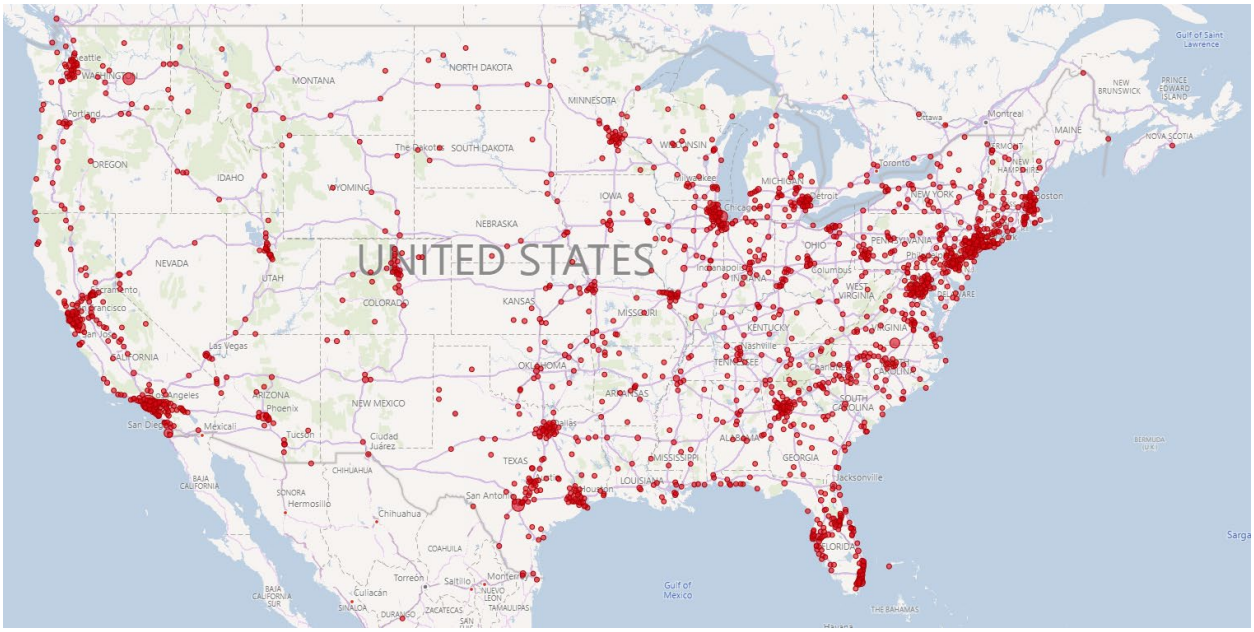


FIGURE 5 –Cracked Cobalt Strike Victims (US)

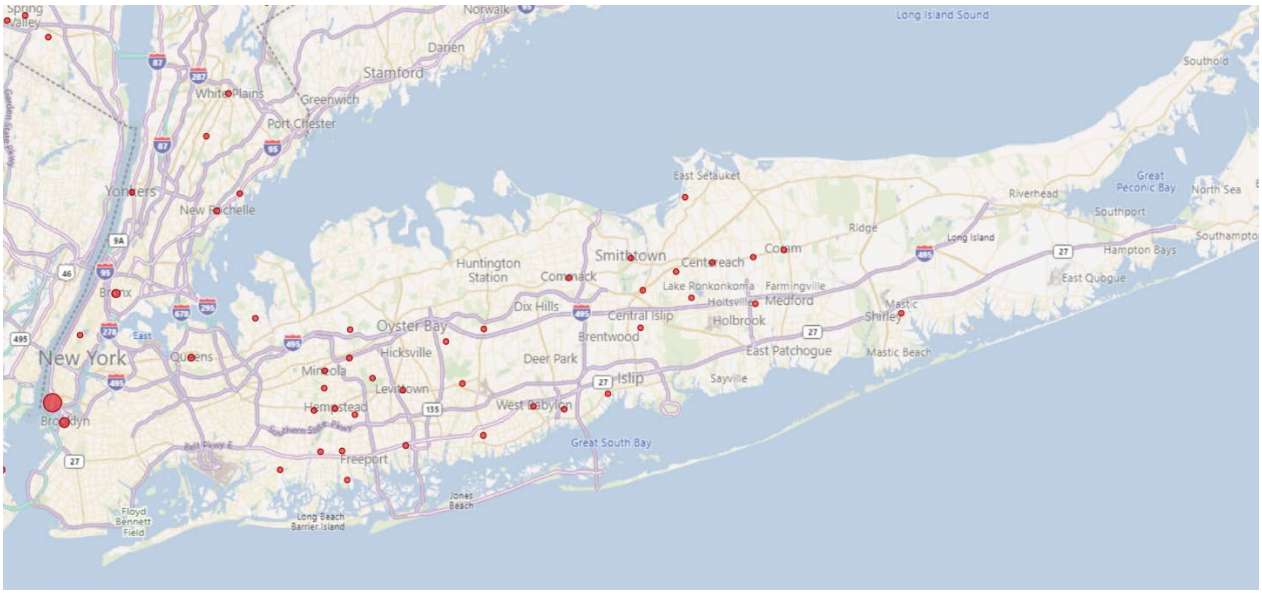


FIGURE 6 – Cracked Cobalt Strike Victims (Eastern District of New York)

IV. RANSOMWARE FAMILIES DEPLOYED VIA CRACKED VERSIONS OF COBALT STRIKE

24. In analyzing cracked Cobalt Strike, the C2 infrastructure, and the "known malicious" watermarks, I have identified the following ransomware families that are deployed using cracked Cobalt Strike: (1) Conti (2) LockBit, (3) Quantum Locker, (4) Royal, (5) Cuba, (6) BlackBasta, (7) BlackCat, and (8) PlayCrypt.

25. In connection with this investigation, DCU did a full analysis of the Conti and LockBit ransomware families. For a description of the methodology of the API analysis conducted, *see* the Declaration of Rodel Finones filed concurrently with Plaintiffs' Application for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction ("Finones Decl.") ¶¶ 28-36.

26. Cracked versions of Cobalt Strike have been leveraged by actor groups deploying the Conti ransomware. One of the more high-profile attacks was in April 11, 2022, when the Conti group leveraged Cobalt Strike—specifically, the cracked version of Cobalt Strike that investigators have associated with the 57117187 watermark—in an attack against the Costa Rican government. The April cyberattack forced the government to declare a state of emergency on May 8, 2022. *See* Ionut Ilascu, *How Conti Ransomware Hacked and Encrypted the Costa Rican Government*, BLEEPING COMPUTER (Jul. 21, 2022)[5]; *see also* Costa Rican Government Victim Impact Statement attached to this declaration as **Exhibit 2**.

27. The relationship between the Conti ransomware and cracked Cobalt Strike is well documented. *See, e.g.*, Charlotte Hammon, Ole Villadsen, Golo Muhr, *ITG23 Crypters Highlight Cooperation Between Cybercriminal Groups*, Security Intelligence (May 19, 2022)[6] (describing the use of cracked Cobalt Strike by bad actors in connection with various Conti attacks and general coordination and cooperation between cybercriminal groups); Microsoft Defender Threat

[5] Available at https://www.bleepingcomputer.com/news/security/how-conti-ransomware-hacked-and-encrypted-the-costa-rican-government/
[6] Available at https://securityintelligence.com/posts/itg23-crypters-cooperation-between-cybercriminal-groups/

Intelligence & Microsoft Threat Intelligence Center (MSTIC), *Ransomware as a Service: Understanding the Cybercrime Gig Economy and How to Protect Yourself* Microsoft Security Blog (May 9, 2022)[7] (bad actors who operate as a Ransomware as a Service (RaaS) deploy cracked versions of Cobalt Strike in connection with ransomware attacks, including Conti, to avoid detection and remain a resident in the infiltrated network longer.

28. Conti is an incredibly dangerous and damaging ransomware. Once the Conti ransomware is deployed and executed on a victim's device, a variety of actions involving dynamic link libraries (dll) and application programming interfaces (APIs) take place. Windows dlls are files that contain preprogramed instructions that other programs can call upon to take defined actions, and APIs are interfaces that allow computer programmers to build new applications on top of other software components and access the functionality of published software modules and services on the web. Once the Conti ransomware is on the victim's system, the Windows dlls are loaded, but the API addresses are not resolved until they are needed by the ransomware. Per previously examined data, the Conti ransomware will call different APIs depending on the path that it follows, and this may vary depending on the target. For the Conti ransomware to use an API, the ransomware must first load the appropriate library, then resolve the API, and provide the necessary parameters to make the API calls. The list of initial dlls resolved are standard on Windows machines, and those initial dlls can usually be found in the Windows system directory.

29. Conti has hard-coded flags that can take multiple values, for example, they have a hard-coded flag that indicates if there are remote machines; and if so, the ransomware will attempt to encrypt those machines. Similarly, the Conti ransomware is coded to look for internal IP addresses, within the internal network, as these are most likely the addresses of the machines that Conti can reach, infect, and encrypt. Part of the danger of the Conti ransomware is the speed at which the ransomware encrypts. The faster the encryption is done, the less time there is for detection making it harder for an investigator to analyze multiple threads on the victim's system.

[7] Available at https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

Similarly, the faster encryption is done, the less time there is between a possible Endpoint Detection and Response (EDR) or Antivirus (AV) detection and completion of encryption.

30. Conti ransomware is sophisticated. It is designed to delete any backups of the data they plan to encrypt so the victim cannot recover the data without paying the ransom. The Conti ransomware is careful not to encrypt directories that may corrupt the system so they are ignored. After the desired files are encrypted and the backups are deleted, the ransomware note is then decrypted and written into each directory encrypted by the Conti as a readme.txt file. The note is hard-coded into the ransomware body and contains the ransom demands. The figure below depicts the flow of a Conti ransomware attack.

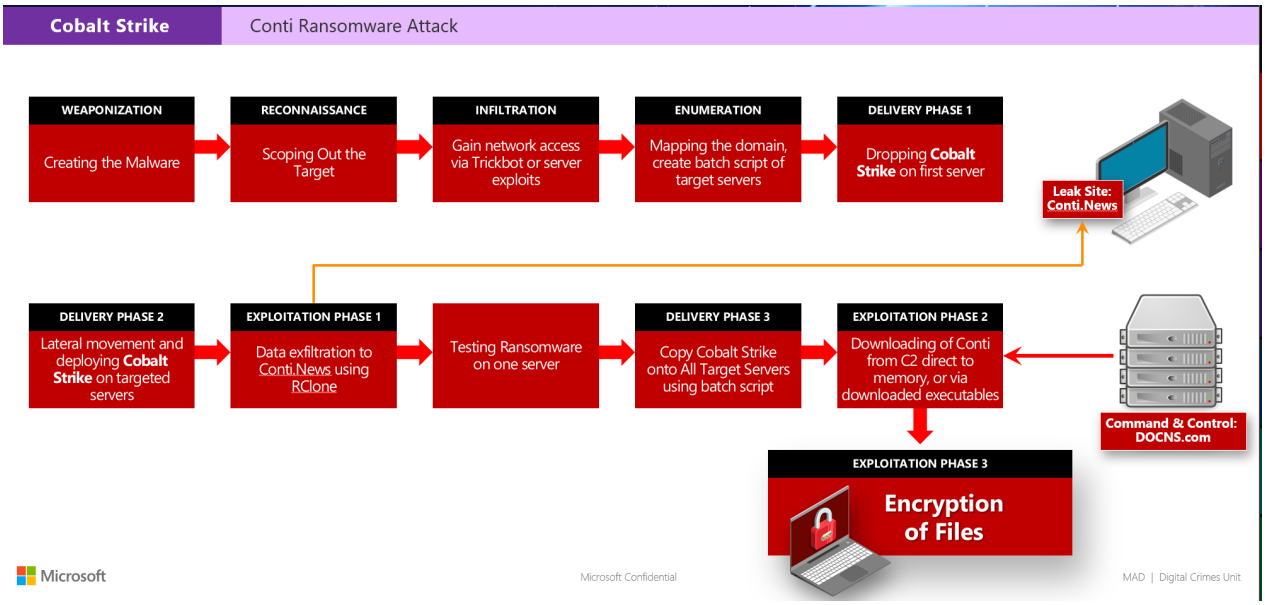


FIGURE 7 – Conti Ransomware Attack

31. Similarly, LockBit is another ransomware family that utilizes Cobalt Strike in its attack chain. *See* Julio Dantas, James Haughom, and Julien Reisdorffer, *Living Off Windows Defender | LockBit Ransomware Sideloads Cobalt Strike Through Microsoft Security Tool*, SentinelOne Blog (Jul. 28, 2022)[8] (Criminal actors deploying LockBit, which is another iteration

[8] Available at https://www.sentinelone.com/blog/living-off-windows-defender-lockbit-ransomware-sideloads-cobalt-strike-through-microsoft-security-tool/

of the increasingly prevalent RaaS, have been abusing Windows Defender command lines to leverage cracked Cobalt Strike for deployment and to avoid detection).

32. LockBit is a ransomware family that was first detected in September 2019. *See* MSTIC, *Ransom:Win32/LockBit*, MICROSOFT, Oct. 6, 2020[9] (describing LockBit as "ransomware [that] encrypts the data on your disk and can stop you from using your device or accessing your data. It encrypts files, renders them inaccessible, and demands payment for the decryption key.") Later iterations of LockBit (LockBit 2.0 and 3.0) have increased sophistication: the "fastest encryption software" in the world, the ability to perform DDoS attacks on the victims' infrastructure, the ability to steal sensitive data, and the ability to use leak sites to expose companies' proprietary data. *See* Finones Decl. ¶ 30.

33. Microsoft uses "DEV-####" designations as a temporary name given to an unknown, emerging, or developing cluster of threat activity, allowing it to be tracked as a unique set of information or actors. As discussed further in this declaration, the "Doe" Defendants are associated with several discrete "DEV" groups leveraging cracked Cobalt Strike as part of a common organization and scheme, to carry out attacks via ransomware.[10] One of the criminal attack groups associated with the activity identified in this investigation, DEV-0243, utilized its own cracked version of Cobalt Strike with watermark value 1580103824 to deploy LockBit. The below image demonstrates the attack flow employed by DEV-0243 to use cracked Cobalt Strike to deploy LockBit ransomware.

[9] Available at https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/LockBit

[10] Available at https://www.microsoft.com/en-us/security/blog/2022/11/10/microsoft-threat-intelligence-presented-at-cyberwarcon-2022/

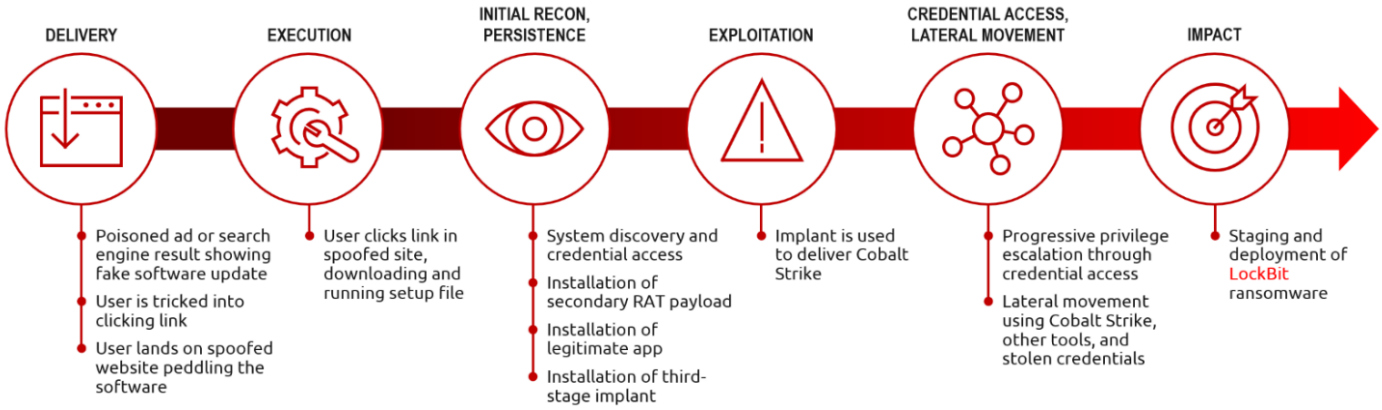


FIGURE 8 – DEV-0243 Attack Flow Using Cracked Cobalt Strike

34. Access to the victims is obtained using fake software updates that install malware on the victims' computers. Subsequently, cracked versions of Cobalt Strike are installed. Once installed, this allows the threat actors to have access to information regarding the victims' computer infrastructure, such as the ability to monitor, escalate privileges through credential access, move laterally within the network, and stage and deploy LockBit ransomware. The attackers can then extort the victims (either by deploying ransomware, which causes downtime until the victim pays the ransom or by directing deleting cloud resources and continuing such deletion until they are paid).

35. LockBit 2.0 (the iteration of LockBit that has been active since June 2021) is considered the most impactful RaaS for five consecutive months. *See* Amer Esad, Jr Gumarin and Abigail Barr, *Lockbit 2.0: How This Raas Operates and How to Protect Against It*, UNIT 42 BY PALO ALTO NETWORKS (Jun. 9, 2022).[11] Specifically, as of May 2022, LockBit 2.0 accounted for forty-six percent of all ransomware-related breach events for 2022 (Conti, by comparison was responsible for approximately twenty-two percent of ransomware-related breach events during the same time period). *Id.* Threat actors using LockBit have boasted that they infected and demanded ransom from over 12,000 companies. *Id.* As of 2022, fifty percent of the

[11] Available at https://unit42.paloaltonetworks.com/lockbit-2-ransomware/

victims of LockBit attacks are located in the United States.

V. DEFENDANTS' CRACKED VERSIONS OF COBALT STRIKE, ASSOCIATED INFRASTRUCTURE AND ASSOCIATED RANSOMWARE ACTIVITY ARE PART OF AN ORGANIZED, CONTINUING AND COMMON OPERATION

36. I have observed cracked, cracked versions of Cobalt Strike, the infrastructure at issue and associated ransomware attacks being linked to the following criminal actor groups, each associated with the "Doe" Defendants in this case:

JOHN DOES	THREAT GROUP	FUNCTION
John Does 1-2	Actors responsible for cracked Cobalt Strike infrastructure for use by malicious actors, including the remaining Defendants, collectively referred to in this matter as John Does 1-2	Cracked Cobalt Strike proliferation, providing infrastructure as a service for cybercriminals.
John Does 3-4	Actors responsible for ransomware associated with cracked Cobalt Strike, collectively referred to in this matter as John Does 3-4	Conti ransomware proliferation after compromise using cracked Cobalt Strike.
John Does 5-6	Actors responsible for ransomware associated with cracked Cobalt Strike, collectively referred to in this matter as Does 5-6	LockBit ransomware proliferation after compromise using cracked Cobalt Strike.
John Does 7-8	DEV-0193 are actors responsible for ransomware associated with cracked Cobalt Strike, collectively referred to in this matter as Does 7-8	Develops, distributes, and manages many different payloads, including Trickbot, Bazaloader, and AnchorDNS. Also manages ransomware as a service (RaaS) programs that are developed as a result of leveraging cracked Cobalt Strike Beacons to drop ransomware payloads.
John Does 9-10	DEV-0206 are actors responsible for providing access to victim computers using cracked	Access broker that uses malvertising technique to gain access to and profile networks using Cobalt Strike payloads and in numerous instances, led to custom cracked Cobalt Strike loaders created by

JOHN DOES	THREAT GROUP	FUNCTION
	Cobalt Strike, collectively referred to in this matter as Does 9-10	malware families. This group offers access for purchase, often using cracked Cobalt Strike payloads.
John Does 11-12	DEV-0237 are actors responsible for ransomware associated with cracked Cobalt Strike, collectively referred to in this matter as Does 11-12	Prolific RaaS affiliate that alternates between different payloads in their operations based on what is available. Uses the cybercriminal gig economy to also gain initial access to networks. Leverages cracked Cobalt Strike Beacons dropped by the malware they purchased to conduct reconnaissance. This group has been responsible for many publicly documented Ryuk and Conti incidents and tradecraft.
John Does 13-14	DEV-0243 are actors responsible for providing custom, cracked Cobalt Strike loaders, collectively referred to in this matter as Does 13-14	"EvilCorp" group that develops Cobalt Strike loaders for other malware campaigns. This group is responsible for providing custom cracked Cobalt Strike loaders for a ransomware payload.
John Does 15-16	DEV-0504 are actors responsible for ransomware associated with cracked Cobalt Strike, collectively referred to in this matter as Does 15-16	Relies on access brokers to enter a network, using Cobalt Strike beacons they purchased access to, to move laterally and stage their payloads. They frequently disable antivirus products that are not protected with tamper protection. This group has been associated with the "REvil gang" or "BlackCat ransomware group"

37. The above Defendants have leveraged each others' work to create, distribute and operate cracked Cobalt Strike infrastructure, distribute and use customized Cobalt Strike loaders, gain access to victim computers using such infrastructure, and to install ransomware on victim computers and steal money from victims. From the evidence I have reviewed, I conclude that these Defendants have engaged in multiple acts to create, distribute, encourage and operate the infrastructure, loaders and ransomware in a continuous manner, leveraging each others' work and often cooperating significantly to use overlapping cracked Cobalt Strike infrastructure to directly benefit from provisioning that infrastructure or to indirectly benefit from activities carried out

through that infrastructure. The interrelated infrastructure and activities of Defendants have had a continuous structure for at least a year. Over the past twenty-four months, the racketeering activity has increased, likely a direct result of a November 2020 leak of Cobalt Strike source code. *See* Declaration of Jonathan Gross filed concurrently with Plaintiffs' Application for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction, ¶ 13. The relationships between Defendants' infrastructure and activities has been persistent, organized and Defendants operate as a continuing discrete unit and association.

38. From the interrelated nature of the infrastructure and activities of these Defendants, I conclude that the purpose of the cracked Cobalt Strike infrastructure, loaders and associated ransomware is to gain cracked access to victim computers and networks, to gain persistence, to deliver various forms of ransomware and to ultimately steal funds from victims. I conclude from these same facts, upon information and belief, that the Defendants must have known and intended that the cracked Cobalt Strike infrastructure, loaders and associated ransomware was to ultimately extort end-user victims, to gain unauthorized access to their computers and networks, to gain unauthorized access to their financial accounts and funds, and to gain unauthorized access to their stored data and their data in transit, by means of fraudulent pretenses and representations and by means of digital activities transmitted over the Internet. Microsoft has been directly injured in its business and property by these Defendants' acts and their coordinated pattern of acts. Upon information and belief, and my experience in assessing cybercrime threats and victims, I believe that plaintiff Fortra and the healthcare sector members of plaintiff H-ISAC have faced similar threats and injury.

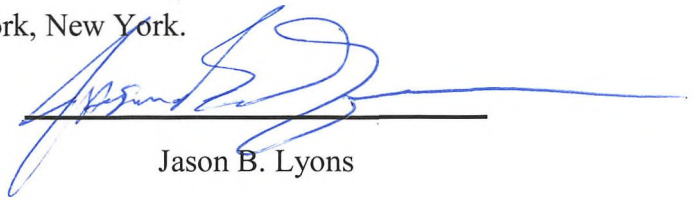
39. From the volume of victim end computers, the resultant value of ransomware attacks on such victims, usually exceeding thousands of dollars per victim, and the value of cracked Cobalt Strike infrastructure provided to other cybercriminal actors, I conclude that each Defendant creator and distributor of cracked Cobalt Strike infrastructure, loaders and ransomware, has obtained payment in a given year of $1,000 or more for such infrastructure or activity.

40. The sale and operation of the cracked Cobalt Strike infrastructure, loaders and

associated ransomware by these Defendants takes place on the Internet, including acts carried out in interstate and international communications and transmissions on and through the Internet.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 30th day of March, 2023, in New York, New York.



Jason B. Lyons

EXHIBIT 1

Jason B. Lyons

802 River Mountain Drive, Boerne, TX 78006
425-894-0061, jasonblyons@gmail.com

SUMMARY

Jason Lyons is an experienced investigator specializing in computer investigations. Trained and experienced in hacker methodology/techniques, computer forensics, incident response, electronic discovery, litigation support and network intrusion investigations.

SECURITY CLEARANCE

- Top Secret/SCI-Expired.

CERTIFICATIONS

- Encase Certified Examiner (EnCE) - Guidance Software
- Counterintelligence Special Agent - Department of the Army
- Certified Basic Digital Media Collector - Department of Defense
- Certified Basic Computer Crime Investigator – Department of Defense
- Certified Basic Digital Forensic Examiner – Department of Defense
- State of Texas licensed Private Investigator

TECHNICAL SKILLS

- **Network Intrusion Investigations**
- **Computer Forensics**
- **Incident Response**
- **EnCase Certified Examiner**
- **Investigative Network Monitoring**
- **PDA and Cell Phone Seizure and Forensics**
- **Investigation Management/Liaison**
- **Expert Witness Experience**
- **Computer Media Evidence Collection**
- **Technical/Investigative Report Writing**

PROFESSIONAL EXPERIENCE

2013-Present Microsoft
Digital Crimes Unit (DCU)
Senior Manager of Investigations

- Work with public (law enforcement, country certs) and private sectors, and develop international partnerships to support malware disruptions on a global scale.
- Conduct proactive malware investigations to identify critical command control infrastructure and to develop disruption strategy to eliminate or severely cripple cyber-criminal infrastructure.
- Document and identify monetization schemes utilized by cyber-criminals ranging from online advertising fraud, ransomware, and targeted financial fraud.
- Work with the Microsoft legal team to develop new legal strategies to disrupt cyber crime through both civil and criminal proceedings.
- Collect electronic evidence to support global malware disruptions and develop criminal referrals for law enforcement.
- Enhance Microsoft's Cyber Threat Intelligence Program (CTIP) which empowers ISP and country CERTS too identify victims of cybercrime.
- Provide expert court testimony with the support of written declarations describing the threat and impact of malware threats on the Microsoft ecosystems.
- Lead and participate in security community working groups that support cybercrime disruption.

- Work with Microsoft Malware Protection Center (MMPC), and other Anti-Virus vendors, to enhance detection of malware and to assist in the development of disruption strategies.

2005 – 2013 ***Affiliated Computer Services, inc (ACS)***
Digital Forensic and eDiscovery Group
Manager of the Digital Forensics Group (DFG)

- Manager of a fortune 500 company's digital forensic laboratory/group. Responsible for managing, coordinating, investigating, and reporting on legal, corporate security, human resources, and ethics investigations involving digital media.
- Developed policy and procedures for digital evidence acquisition, storage, examination, processing and production.
- Developed and maintained technical investigative support for ACS inside and outside legal counsel on eDiscovery matters. Experienced in developing and executing large eDiscovery collection plans, preserving data in a forensically sound manner, culling of relevant data, presenting data for review, hosting data for review, and producing relevant data for final production.
- Implemented Access Data's Enterprise and eDiscovery solution.

2003 – 2005 ***Department of the Army, 902nd Military Intelligence (MI),***
Cyber Counterintelligence Activity (CCA)
Assistant Operations Officer/Counterintelligence Special Agent

- Assisted in managing of all CCA branch operations to include all cyber investigations, special intelligence collection missions, cyber investigator training, and quality assurance of all investigative products.
- Supervised 35 special agents and computer forensic technicians.
- Prepared detailed investigative briefings which include results of investigations and forensic analysis for executive level officers.
- Conducted national level liaisons with federal intelligence and law enforcement agencies on many national security investigations.
- Conducted network intrusion investigations, computer media forensics examinations, counterintelligence/counterterrorism special operations, and network forensic analysis.

2000 – 2003 ***Department of the Army, 902nd MI, CCA***
Counterintelligence Special Agent / Computer Investigator

- Assistant Supervisory Special Agent (ASSA) of an eight man computer Incident Response Team (IRT) specializing in cyber investigations.
- Accountable for managing, editing and reviewing associated technical and investigative reports pertaining to the IRT's investigations.
- Provided and maintained incident response, computer forensics, evidence handling, and computer media search and seizure training for the members of the IRT.
- While assigned to the IRT, served as lead agent on numerous network intrusion and computer forensic Counterintelligence investigations.

1998-1999 ***Department of the Army, 501st MI Brigade, South Korea***
Counterintelligence Special Agent / Liaison Officer

- Served as liaison officer for a Counterintelligence Resident Office in South Korea.
- Maintained regional-level liaison with foreign government officials to collect strategic information for intelligence reporting.

- Established business partnerships and furthered cooperation between the United States and South Korean investigative/intelligence agencies to accomplish bilateral goals.

EDUCATION

- Graduate from Excelsior College in October 2002, with a Bachelor of Science in Liberal Arts.
- Thirteen hours completed for Masters Degree in Information Technology with University of Maryland University College (UMUC).

TRAINING

- Counterintelligence Agent Course-Department of the Army-1998.
- Counterintelligence Fundamentals Warfare (CIFIW)-Department of the Army-2000.
- Introduction to Computer Search and Seizure-Defense Computer Investigation Training Program (DCITP), Linthicum, MD-2000.
- Introduction to Networks and Computer Hardware (INCH)-DCITP, Linthicum, MD-2000.
- Network Intrusion Analysis Course (NIAC)-DCITP, Linthicum, MD-2001.
- Computer Investigations for Special Agents (CICSA)-Department of the Army-2001.
- Basic Evidence Recovery Techniques (BERT)-DCITP, Linthicum, MD- 2002.
- Basic Forensic Examiner Course (BFE)-DCITP-Linthicum, MD-2002.
- Forensics in a Solaris Environment (FISE)-DCITP-Linthicum, MD-2002.
- SANS-Tracking Hackers/Honey pots-SANS Institute, Dupont Circle, DC-2003.
- Encase Intermediate Analysis and Reporting-Guidance Software, Sterling VA-2004.
- PDA and Cell Phone Seizure and Analysis-Paraben Software, Orlando FL-2005
- Network Monitoring Course (NMC)-DCITP- Linthicum, MD-2005
- Encase Advanced Internet Examinations-Guidance Software, Los Angeles CA-2006
- (FTK) Windows Forensics-AccessData, Dallas TX-2006
- (DNA) Applied Decryption-AccessData, Nashville TN, 2007
- Network Intrusion Course-Guidance Software, Houston, TX, 2010
- SANS-Hacker Techniques, Exploits, and Incident Handling, San Francisco, CA, 2011

EXHIBIT 2

2022-2026 COSTA RICA TRABAJANDO, DECIDIENDO, MEJORANDO

micitt MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

Febrero 2,2023

Señores,
Microsoft Corp
Presente. -

Atención: Marlon Fetzner-Jimena Mora

Asunto: Ciberataques Costa Rica, abril -junio 2022

A nivel mundial se reconoce que las tecnologías digitales (TD) y en especial las tecnologías de la información y la comunicación (TIC) son un catalizador para el desarrollo económico, social y cultural, dado que facilitan el acceso a incalculables recursos que además de la comunicación, promueven la innovación, la eficiencia, la transparencia, y la prosperidad socioeconómica de los países.

Costa Rica, consciente de ello, ha apostado por una fuerte promoción del uso de las TIC para impulsar el desarrollo nacional y consolidar una sociedad de la información y el conocimiento preparada para enfrentar los desafíos de la cuarta revolución industrial y la transformación digital. De ello, son reflejo la Política Nacional de Sociedad y Economía Basada en el Conocimiento 2022-2050 (PNSEBC), el Plan Nacional de Ciencia, Tecnología e Innovación 2022-2027 (PNCTI)y la Estrategia de Transformación Digital(2017-2022), esto último, en proceso de actualización consulta, entre otras. Sin embargo, con los altos índices de conectividad y acceso a las TIC, la apuesta por la digitalización del Gobierno, el almacenamiento masivo de datos sensibles, y la acelerada transformación impulsada por la pandemia, surgen riesgos y vulnerabilidades propias del ciberespacio que exponen a todos los sectores de la sociedad a consecuencias perjudiciales.

El resultado de esta transición hacia lo digital es un extraordinario aumento de ataques cibernéticos, en todo el mundo, incluida Costa Rica. La administración pública sufrió ataques cibernéticos significativos durante los meses de abril, mayo y junio del año 2022, a casi una treintena de instituciones públicas, esta situación provocó una declaratoria de emergencia nacional de parte del Poder Ejecutivo, que en ningún otro país en la región se había dado. Estos actos fueron dirigidos contra infraestructuras críticas como los sistemas del Ministerio de Hacienda o de la Caja Costarricense del Seguro Social, incluyendo a otras instituciones como el Instituto Meteorológico Nacional, Radiográfica Costarricense, Ministerio de Trabajo, Ministerio de Ciencia, Tecnología, Innovación y Telecomunicaciones (MICITT), Fondo de Desarrollo Social y Asignaciones Familiares(FODESAF) y la Junta Administrativa del Servicio Eléctrico Municipal de Cartago (JASEC), entre otras, comprometiendo con ello la prestación de servicios esenciales

para la población. También, la crisis generada por estos ataques obligó a suspender y dar de baja los sistemas informáticos que soportan la prestación de otros servicios y el cumplimiento de obligaciones a cargo del Estado. o los ingresos de las familias que dependen de esos pagos.

DESCRIPCIÓN DEL EVENTO

De acuerdo con el informe emitido por nuestro Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), el ciberataque al Gobierno de Costa Rica fue un ataque informático de índole extorsivo que se habría iniciado el domingo 17 de abril del 2022 en perjuicio de distintas instituciones públicas de la República de Costa Rica, incluido el Ministerio de Hacienda, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), el Instituto Meteorológico Nacional (IMN), la Radiográfica Costarricense Sociedad Anónima (RACSA), el Ministerio de Trabajo y Seguridad Social (MTSS), el Fondo de Desarrollo Social y Asignaciones Familiares (FODESAF) y la Junta Administrativa del Servicio Eléctrico Municipal de Cartago (JASEC), la Caja Costarricense del Seguro Social (CCSS).

El grupo de origen ruso Conti (también conocido como Wizard Spider, TrickBot, Ryuk, UNC1878 y Karakurt) se atribuyó el ciberataque (a excepción del caso de la CCSS que fue un incidente en sus redes sociales y en sus bases de datos que CONTI no se atribuyó) y solicitó un rescate de 10 millones de dólares estadounidenses a cambio de no liberar la información sustraída del Ministerio de Hacienda, la cual podría incluir información sensible como las declaraciones de impuestos de los ciudadanos y empresas que operan en Costa Rica. Conti es una organización criminal de origen ruso dedicada a realizar ataques de ransomware por medio de la infección de equipos y servidores, sustrayendo archivos y documentos de servidores para luego exigir un rescate. Conti es capaz de obtener acceso inicial sobre las redes de sus víctimas a través de distintas técnicas. Por ejemplo:

- Campañas de phishing especialmente dirigidas que contienen documentos adjuntos maliciosos (como un archivo Word) o enlaces. Estos adjuntos descargan malware como TrickBot, Bazar backdoor o incluso aplicaciones legítimas como Cobalt Strike que son utilizadas de forma maliciosa para realizar movimiento lateral dentro de la red de la víctima y luego descargar el ransomware.
- Explotación de vulnerabilidades conocidas sobre equipos que están expuestos a Internet.
- Ataques sobre equipos con el servicio de RDP (Protocolo de Escritorio Remoto) expuesto a Internet.
- Todas las acciones realizadas por este grupo cibercriminal forman parte de un evento imprevisible que impidió el desarrollo de las labores habituales de servicios al público, de las instituciones del Estado involucradas, por medio de sus plataformas tecnológicas, siendo que las medidas existentes de ciberseguridad, ante las acciones de este grupo especializado de cibercrimen, hicieron inevitable la situación presentada.

Las consecuencias reportadas al MICITT por las instituciones afectadas fueron:

- En el caso del Ministerio de Educación: la suspensión del sistema "Integra 2", que habría generado dificultades para el pago de los salarios de 13 mil funcionarios de esa institución.

- Sólo en las primeras 48 horas de hackeo en los sistemas de aduanas del Ministerio de Hacienda, provocaron pérdidas que rondan los $125 millones, según datos de la Cámara de Comercio Exterior (Crecex)

- En la Caja Costarricense del Seguro Social (CCSS) : Como medidas de protección se bloquearon los direccionamientos desde otros países producto del ataque, en los dispositivos de seguridad. Así mismo se baja el portal RRHH para que no pueda ser accedido al externo (sitio web). Lo que ocasiono que los ciudadanos no pudieran tener el servicio de salud de manera continua por un periodo de tiempo.
- En el Ministerio de Hacienda: la afectación de servicios para la recolección de tributos emisión de facturas, entre otros

Puede consultar la información del Plan General de Emergencias ante el CiberAtaque en el siguiente link https://www.cne.go.cr/recuperacion/declaratoria/planes/Plan%20General%20de%20la%20Emergencia%20por%20Ciberataques.pdf

Como se menciona, estos ataques ocasionaron graves afectaciones a la prestación de servicios esenciales por parte del Estado. La presente comunicación tiene como objetivo colaborar con la disrupción de las redes criminales informáticas que pudieron ser partícipes de esta situación, así como prevenir la afectación en otras víctimas, instituciones y Estados.

Lamentablemente, hemos seguido siendo víctimas de los ataques a entidades del Estado, reporto a continuación:

Ministerio de Obras Públicas y Transportes
https://delfino.cr/2023/01/nuevo-ciberataque-deja-12-servidores-del-mopt-encriptados-confirma-micitt

Ministerio de Salud
https://observador.cr/ministerio-de-salud-sufre-hackeo-que-se-encuentra-contenido-y-en-investigacion/

Cordialmente,

Paula Francheska Brenes Ramírez
Directora de Gobernanza Digital
Ministerio de Ciencia, Tecnología y Telecomunicaciones Costa Rica

English Transalation of Costa Rica Victim Statement[1]

February 2,2023

Srs,
Microsoft Corp

Present. -

Attention: Marlon Fetzner-Jimena Mora
Subject: Cyberattacks Costa Rica, April-June 2022

At the global level, it is recognized that digital technologies (DT) and especially information and communication technologies (ICTs) are a catalyst for economic, social, and cultural development, since they facilitate access to incalculable resources that, in addition to communication, promote innovation, efficiency, transparency, and socioeconomic prosperity of countries.

Costa Rica, aware of this, has opted for a strong promotion of the use of ICTs to boost national development and consolidate an information and knowledge society prepared to face the challenges of the fourth industrial revolution and digital transformation. This is reflected in the National Policy on Society and Knowledge-Based Economy 2022-2050 (PNSEBC), the National Science, Technology, and Innovation Plan 2022-2027 (PNCTI) and the Digital Transformation Strategy (2017-2022), the latter, in the process of updating consultation, among others. However, with the high rates of connectivity and access to ICTs, the Government's commitment to digitalization, the massive storage of sensitive data, and the accelerated transformation driven by the pandemic, risks and vulnerabilities of cyberspace arise that expose all sectors of society to harmful consequences.

The result of this transition to digital is an extraordinary increase in cyberattacks, around the world, including Costa Rica. The public administration suffered significant cyber attacks during the months of April, May and June of the year 2022, to almost thirty public institutions, this situation caused a declaration of national emergency by the Executive

[1] The English translation of this letter was provide by Jimena Mora Corredor, a Microsoft attorney who is based in Latin American and is a native Spanish speaker. Ms. Mora-Corredor was the recipient of this letter from Paula Francheska Brenes Ramírez, Digital Governance Director, Ministry of Science, Technology and Telecommunications of Costa Rica.

Power, which in no other country in the region had occurred. These acts were directed against critical infrastructures such as the systems of the Ministry of Finance or the Costa Rican Social Security Fund, including other institutions such as the National Meteorological Institute, Costa Rican Radiographic, Ministry of Labor, Ministry of Science, Technology, Innovation and Telecommunications (MICITT), Social Development and Family Allowances Fund (FODESAF) and the Administrative Board of the Municipal Electric Service of Cartago (JASEC). among others, thereby compromising the provision of essential services.

DESCRIPTION OF THE EVENT

According to the report issued by our Ministry of Science, Technology and Telecommunications (MICITT), the cyberattack on the Government of Costa Rica was a computer attack of an extortion nature that would have begun on Sunday, April 17, 2022 to the detriment of different public institutions of the Republic of Costa Rica, including the Ministry of Finance, the Ministry of Science, Innovation, Technology and Telecommunications (MICITT), the National Meteorological Institute (IMN), the Costa Rican Radiographic Company (RACSA), the Ministry of Labour and Social Security (MTSS), the Social Development and Family Allowances Fund (FODESAF) and the Administrative Board of the Municipal Electric Service of Cartago (JASEC), the Costa Rican Social Security Fund (CCSS).

The group of Russian origin Conti (also known as Wizard Spider, TrickBot, Ryuk, UNC1878 and Karakurt) claimed responsibility for the cyberattack (except for the case of the CCSS that was an incident in their social networks and in their databases that CONTI did not attribute) and requested a ransom of 10 million US dollars in exchange for not releasing the stolen information from the Ministry of Finance, which could include sensitive information such as tax returns of citizens and companies operating in Costa Rica. Conti is a criminal organization of Russian origin dedicated to carrying out ransomware attacks by infecting computers and servers, stealing files and documents from servers and then demanding a ransom. Conti is able to gain initial access to his victims' networks through different techniques. For example:

- Specially targeted phishing campaigns containing malicious attachments (such as a Word file) or links. These attachments download malware like TrickBot, Backdoor Bazaar or even legitimate apps like Cobalt Strike that are maliciously used to perform lateral movement within the victim's network and then download the ransomware.
- Exploitation of known vulnerabilities on computers that are exposed to the Internet.
- Attacks on computers with the RDP (Remote Desktop Protocol) service exposed to the Internet.

- All the actions carried out by this cybercriminal group are part of an unforeseeable event that prevented the provision of services by the public entities involves to the public, through their technological platforms, being that the existing cybersecurity measures, before the actions of this specialized group of cybercrimes, made the situation presented inevitable.

The consequences reported to MICITT by the affected institutions were:

- In the case of the Ministry of Education: the suspension of the "Integra 2" system would have generated difficulties in paying the salaries of 13,000 officials of that institution.
- Only in the first 48 hours of hacking in the customs systems of the Ministry of Finance, they caused losses of around $ 125 million, according to data from the Chamber of Foreign Trade (Crecex)
- In the Costa Rican Social Security Fund (CCSS): As protection measures, addresses from other countries were blocked because of the attack, in security devices. Likewise, the HR portal is downloaded so that it cannot be accessed by the external (website). What caused that citizens could not have the health service continuously for a period.
- In the Ministry of Finance: the allocation of services for the collection of taxes issuance of invoices, among others

You can consult the information of the General Emergency Plan before the CyberAttack in the following link:
https://www.cne.go.cr/recuperacion/declaratoria/planes/Plan%20General%20de%20la%20Emergencia%20por%20Ciberataques.pdf

As mentioned, these attacks seriously affected the provision of essential services by the State. The objective of this communication is to collaborate with the disruption of the computer criminal networks that could be participants in this situation, as well as to prevent the affectation of other victims, institutions, and States.

Unfortunately, we have continued to be victims of attacks on state entities, I report below:
Ministry of Public Works and Transport:
https://delfino.cr/2023/01/nuevo-ciberataque-deja-12-servidores-del-mopt-encriptados-confirma-micitt
Ministry of Health :
https://observador.cr/ministerio-de-salud-sufre-hackeo-que-se-encuentra-contenido-y-en-investigacion/

Cordially

Paula Francheska Brenes Ramírez
Digital Governance Director
Ministry of Science, Technology and Telecommunications of Costa Rica