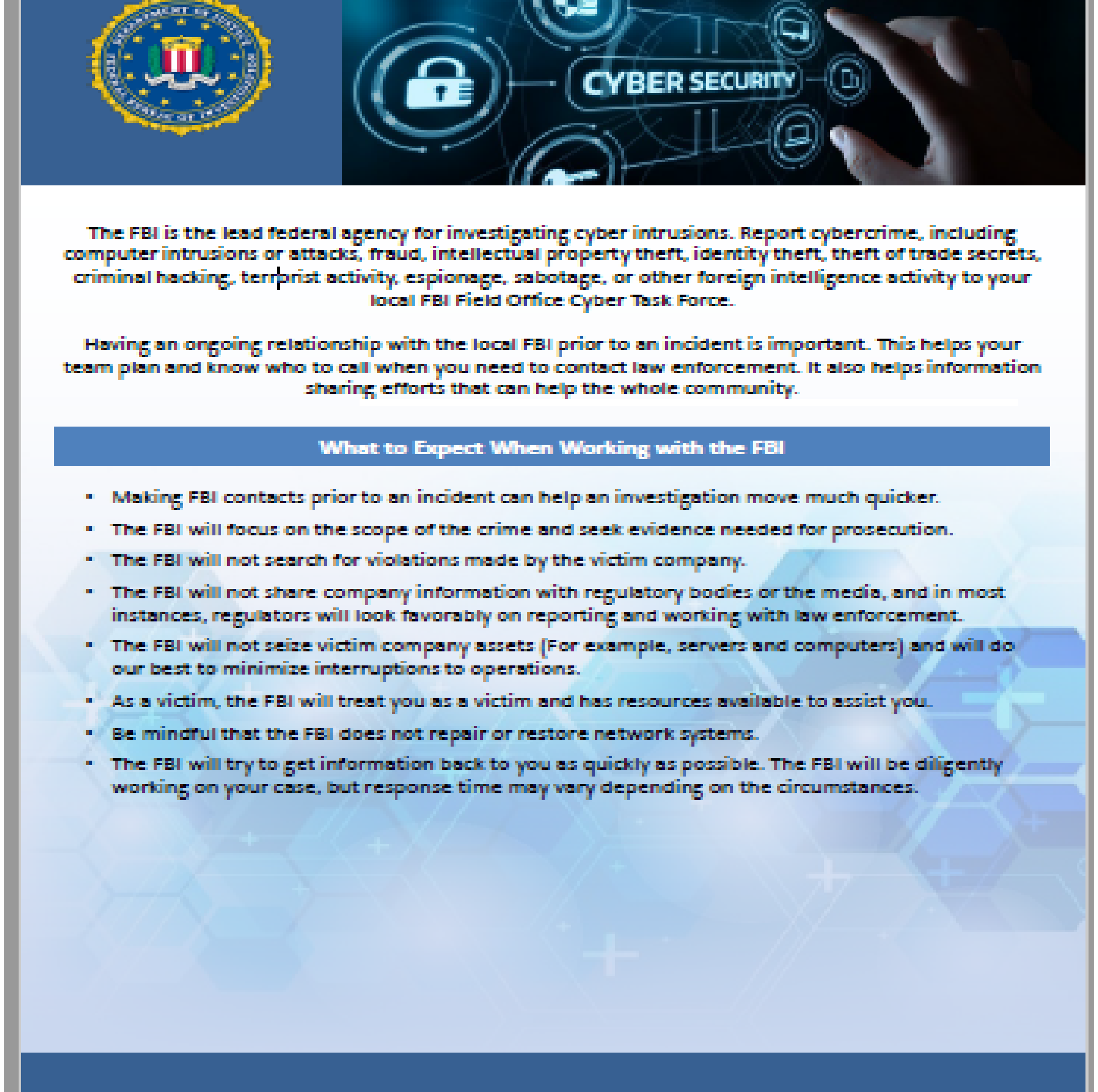


CYBER SECURITY

The FBI is the lead federal agency for investigating cyber intrusions. Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to your local FBI Field Office Cyber Task Force.

Having an ongoing relationship with the local FBI prior to an incident is important. This helps your team plan and know who to call when you need to contact law enforcement. It also helps information sharing efforts that can help the whole community.

What to Expect When Working with the FBI

- Making FBI contacts prior to an incident can help an investigation move much quicker.
- The FBI will focus on the scope of the crime and seek evidence needed for prosecution.
- The FBI will not search for violations made by the victim company.
- The FBI will not share company information with regulatory bodies or the media, and in most instances, regulators will look favorably on reporting and working with law enforcement.
- The FBI will not seize victim company assets (For example, servers and computers) and will do our best to minimize interruptions to operations.
- As a victim, the FBI will treat you as a victim and has resources available to assist you.
- Be mindful that the FBI does not repair or restore network systems.
- The FBI will try to get information back to you as quickly as possible. The FBI will be diligently working on your case, but response time may vary depending on the circumstances.

Preparing for a Cyber Incident

FBI Internet Crime Complaint Center (IC3):
https://www.ic3.gov

Report individual instances of cybercrime to the IC3, which accepts complaints from both victim and third parties.

National Cyber Investigative Joint Task Force (NCIJTF):

24/7 CyWatch Command Center (855) 292-3937 or cywatch@fbi.gov

Although every organization strives to never suffer from a cyber-attack, increasing use of the internet and expanding digital landscape makes it more likely that every organization will one day fall victim to a data breach, ransomware, or other cyber incident.

Preparation, which includes developing an incident response plan, is key to an effective response that minimizes harm and expedites recovery. One way to accomplish that is to establish a point-of-contact with your local FBI field office:

https://www.fbi.gov/contact-us/field-offices

Benefits of Working with the FBI:

- The FBI can respond with a range of investigative assets, all coordinated through the local FBI field office. These include Special Agents, Computer Scientists and Intelligence Analysts in every field office who specialize in computer intrusion investigations. They also include enhanced resources like the Cyber Action Team, a rapid response team of cyber investigation experts who can deploy nearly anywhere in the world to provide advanced digital forensics and incident response capabilities to identify, collect, and analyze the most relevant and immediately actionable evidence of a computer intrusion.

- We pursue investigations that can identify the source of the intrusion and provide context so you understand why you may have been targeted.

- We impose consequences for illicit acts. Consequences include indictment, prosecution, imposition of sanctions, and efforts to name and shame the responsible actors.

A relationship with the FBI can foster information sharing that proves beneficial both to potential victim organizations and law enforcement.

Responding to a Cyber Incident

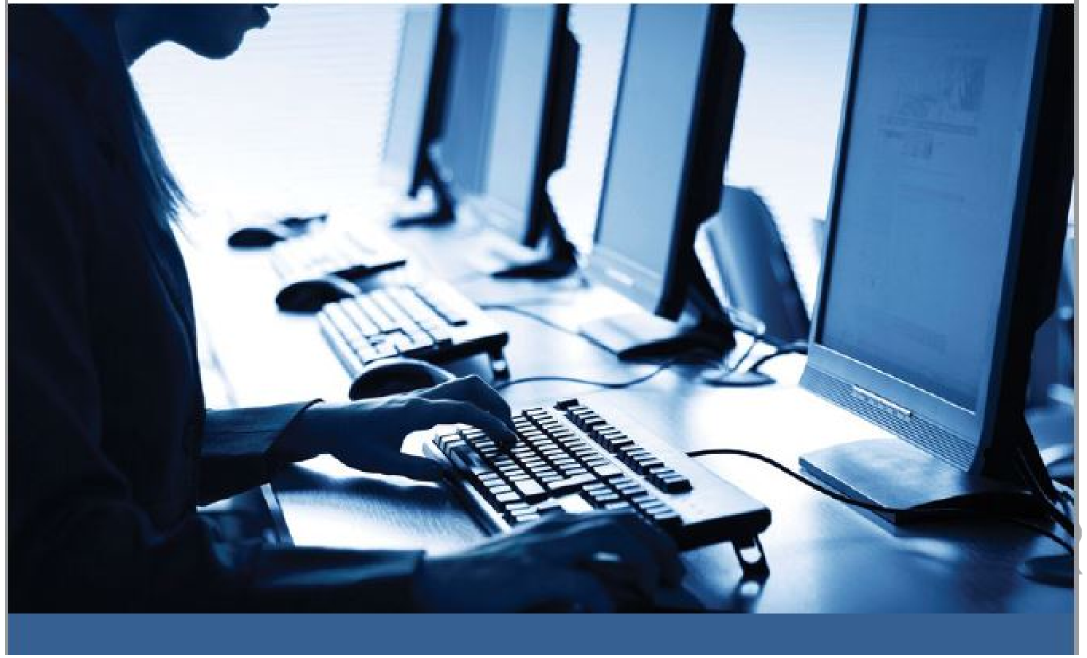
Realities of Working with Law Enforcement:

- We treat victims as victims. Our role is to identify the responsible cyber actors and bring them to justice, not to interfere with your organization's efforts to respond, remediate, and restore operations. Victims are not named in court documents, and charges remain sealed until the responsible party is apprehended. Whenever practicable, protective orders are sought to reduce public disclosure of sensitive information, and exemptions are claimed to guard against any investigative or other sensitive information being released.

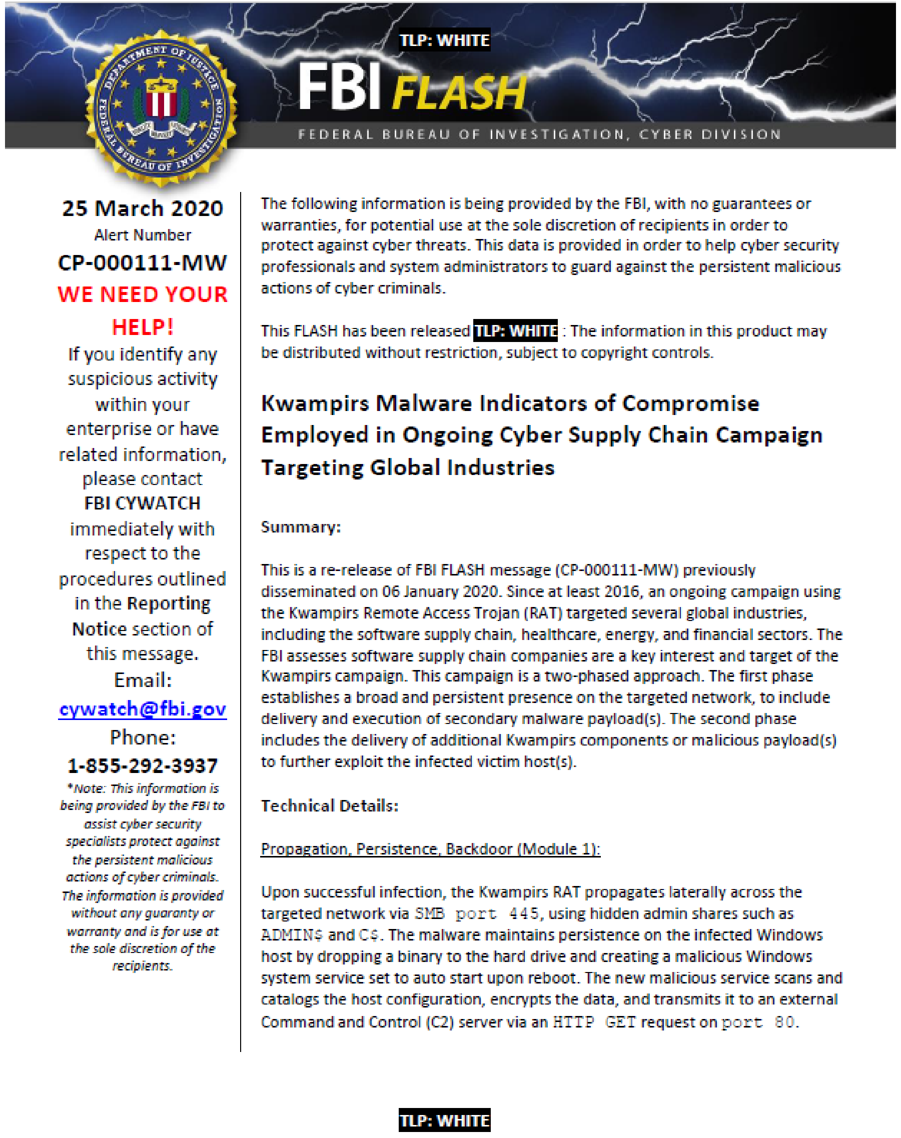
- We strive to minimize disruptions to your business operations. The FBI pursues investigative measures that avoid computer downtime, often seeking only log files and images of affected machines. We also do our best to schedule witness interviews in advance, and avoid displacing employees whenever possible.

- We seek only technical intrusion details, not sensitive internal communications evaluating your company's security. We work closely with incident response firms as permitted by a victim to obtain relevant information for investigative purposes. If evidence is commingled with customer data, we partner with your technical personnel to locate artifacts of the intrusion without sifting through sensitive third party data.

- We are law enforcement, not regulators. As a general rule, we don't share cyber incident information with regulators, and we refer regulators to the victim itself for further information. Indeed, the Federal Trade Commission and Securities & Exchange Commission have stated publicly that they view reporting favorably.



FBI FLASH



TLP: WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

25 March 2020

Alert Number

CP-000111-MW

WE NEED YOUR HELP!

If you identify any suspicious activity within your enterprise or have related information, please contact **FBI CYWATCH** immediately with respect to the procedures outlined in the **Reporting Notice** section of this message.

Email:

cywatch@fbi.gov

Phone:

1-855-292-3937

**Note: This information is being provided by the FBI to assist cyber security specialists protect against the persistent malicious actions of cyber criminals. The information is provided without any guaranty or warranty and is for use at the sole discretion of the recipients.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released **TLP: WHITE** : The information in this product may be distributed without restriction, subject to copyright controls.

Kwampirs Malware Indicators of Compromise Employed in Ongoing Cyber Supply Chain Campaign Targeting Global Industries

Summary:

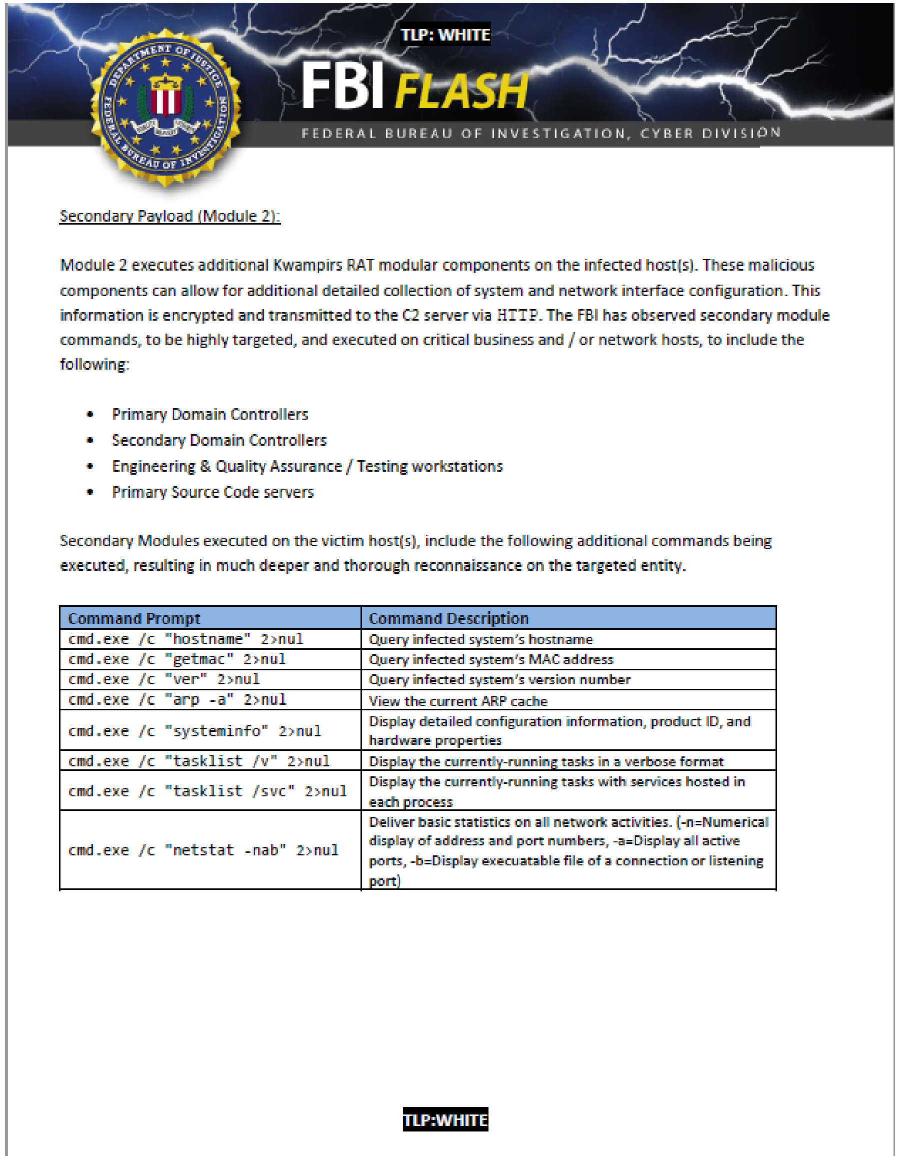
This is a re-release of FBI FLASH message (CP-000111-MW) previously disseminated on 06 January 2020. Since at least 2016, an ongoing campaign using the Kwampirs Remote Access Trojan (RAT) targeted several global industries, including the software supply chain, healthcare, energy, and financial sectors. The FBI assesses software supply chain companies are a key interest and target of the Kwampirs campaign. This campaign is a two-phased approach. The first phase establishes a broad and persistent presence on the targeted network, to include delivery and execution of secondary malware payload(s). The second phase includes the delivery of additional Kwampirs components or malicious payload(s) to further exploit the infected victim host(s).

Technical Details:

Propagation, Persistence, Backdoor (Module 1):

Upon successful infection, the Kwampirs RAT propagates laterally across the targeted network via `SMB port 445`, using hidden admin shares such as `ADMIN$` and `C$`. The malware maintains persistence on the infected Windows host by dropping a binary to the hard drive and creating a malicious Windows system service set to auto start upon reboot. The new malicious service scans and catalogs the host configuration, encrypts the data, and transmits it to an external Command and Control (C2) server via an `HTTP GET` request on `port 80`.

TLP: WHITE



TLP: WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Secondary Payload (Module 2):

Module 2 executes additional Kwampirs RAT modular components on the infected host(s). These malicious components can allow for additional detailed collection of system and network interface configuration. This information is encrypted and transmitted to the C2 server via `HTTP`. The FBI has observed secondary module commands, to be highly targeted, and executed on critical business and / or network hosts, to include the following:

- Primary Domain Controllers
- Secondary Domain Controllers
- Engineering & Quality Assurance / Testing workstations
- Primary Source Code servers

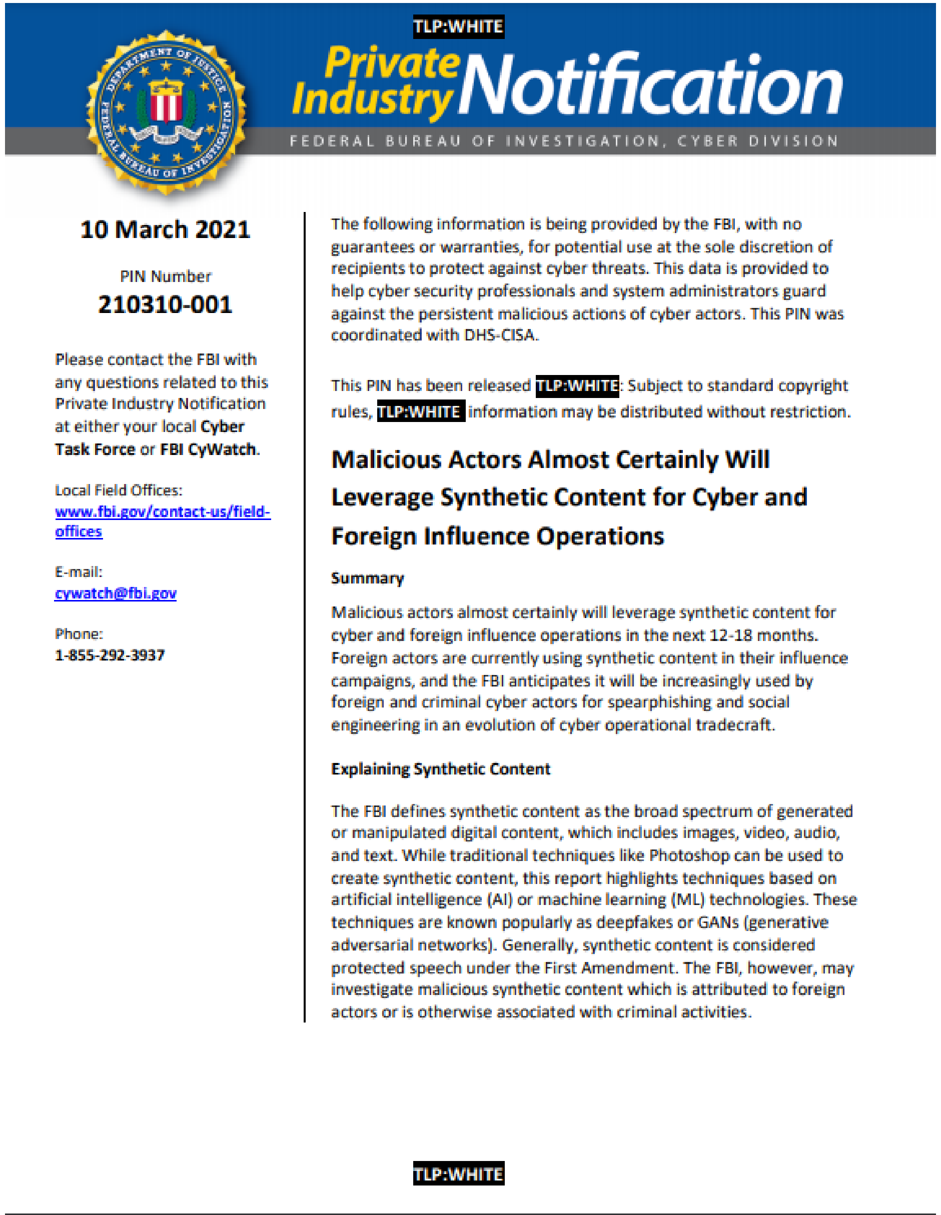
Secondary Modules executed on the victim host(s), include the following additional commands being executed, resulting in much deeper and thorough reconnaissance on the targeted entity.

Command Prompt	Command Description
`cmd.exe /c "hostname" 2>nul`	Query infected system's hostname
`cmd.exe /c "getmac" 2>nul`	Query infected system's MAC address
`cmd.exe /c "ver" 2>nul`	Query infected system's version number
`cmd.exe /c "arp -a" 2>nul`	View the current ARP cache
`cmd.exe /c "systeminfo" 2>nul`	Display detailed configuration information, product ID, and hardware properties
`cmd.exe /c "tasklist /v" 2>nul`	Display the currently-running tasks in a verbose format
`cmd.exe /c "tasklist /svc" 2>nul`	Display the currently-running tasks with services hosted in each process
`cmd.exe /c "netstat -nab" 2>nul`	Deliver basic statistics on all network activities. (-n=Numerical display of address and port numbers, -a=Display all active ports, -b=Display execuatable file of a connection or listening port)

TLP:WHITE

FBI CYBER

FBI PIN



TLP:WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

10 March 2021

PIN Number
210310-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field-offices

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS-CISA.

This PIN has been released **TLP:WHITE**: Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Malicious Actors Almost Certainly Will Leverage Synthetic Content for Cyber and Foreign Influence Operations

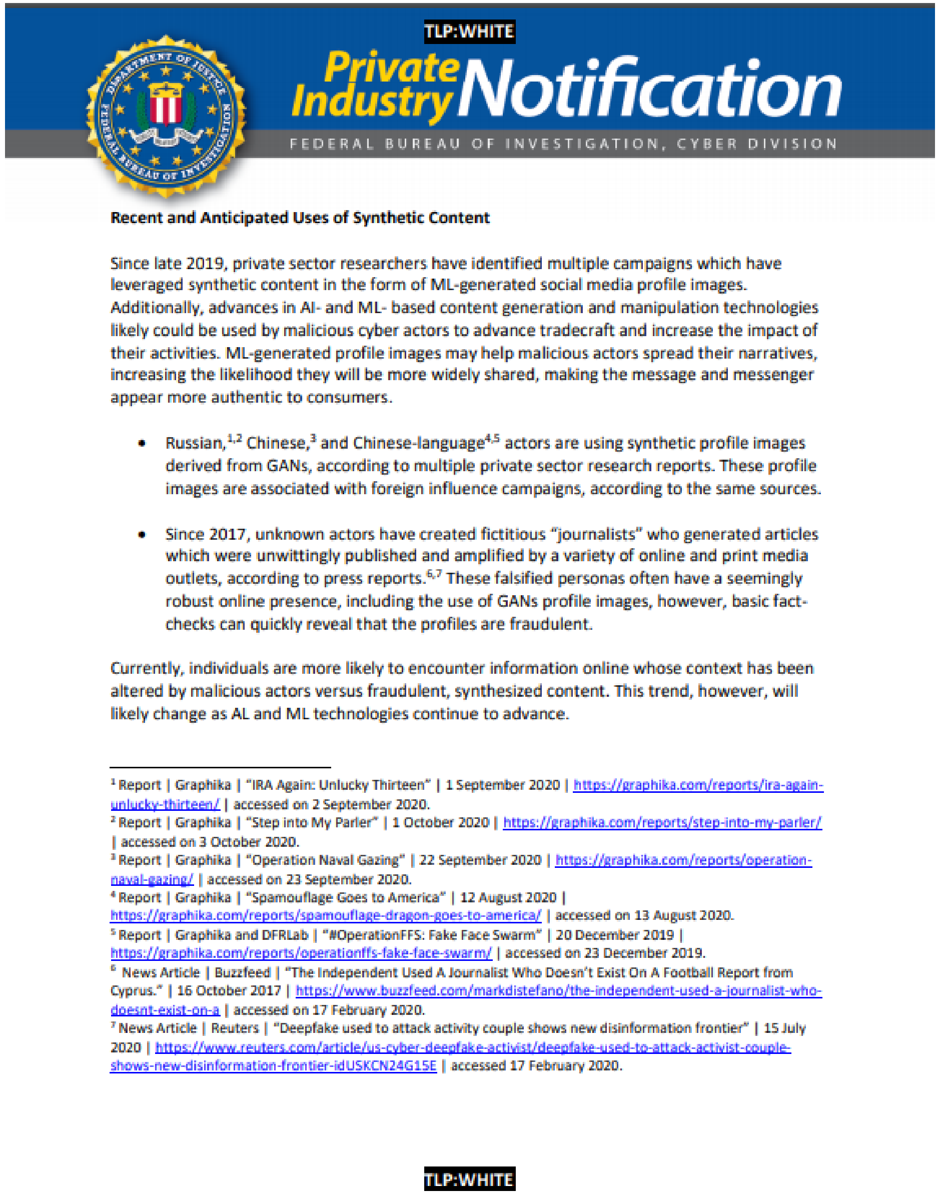
Summary

Malicious actors almost certainly will leverage synthetic content for cyber and foreign influence operations in the next 12-18 months. Foreign actors are currently using synthetic content in their influence campaigns, and the FBI anticipates it will be increasingly used by foreign and criminal cyber actors for spearphishing and social engineering in an evolution of cyber operational tradecraft.

Explaining Synthetic Content

The FBI defines synthetic content as the broad spectrum of generated or manipulated digital content, which includes images, video, audio, and text. While traditional techniques like Photoshop can be used to create synthetic content, this report highlights techniques based on artificial intelligence (AI) or machine learning (ML) technologies. These techniques are known popularly as deepfakes or GANs (generative adversarial networks). Generally, synthetic content is considered protected speech under the First Amendment. The FBI, however, may investigate malicious synthetic content which is attributed to foreign actors or is otherwise associated with criminal activities.

TLP:WHITE



TLP:WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Recent and Anticipated Uses of Synthetic Content

Since late 2019, private sector researchers have identified multiple campaigns which have leveraged synthetic content in the form of ML-generated social media profile images. Additionally, advances in AI- and ML- based content generation and manipulation technologies likely could be used by malicious cyber actors to advance tradecraft and increase the impact of their activities. ML-generated profile images may help malicious actors spread their narratives, increasing the likelihood they will be more widely shared, making the message and messenger appear more authentic to consumers.

- Russian,[1,2] Chinese,[3] and Chinese-language[4,5] actors are using synthetic profile images derived from GANs, according to multiple private sector research reports. These profile images are associated with foreign influence campaigns, according to the same sources.

- Since 2017, unknown actors have created fictitious "journalists" who generated articles which were unwittingly published and amplified by a variety of online and print media outlets, according to press reports.[6,7] These falsified personas often have a seemingly robust online presence, including the use of GANs profile images, however, basic fact-checks can quickly reveal that the profiles are fraudulent.

Currently, individuals are more likely to encounter information online whose context has been altered by malicious actors versus fraudulent, synthesized content. This trend, however, will likely change as AL and ML technologies continue to advance.

[1] Report | Graphika | "IRA Again: Unlucky Thirteen" | 1 September 2020 | https://graphika.com/reports/ira-again-unlucky-thirteen/ | accessed on 2 September 2020.
[2] Report | Graphika | "Step into My Parler" | 1 October 2020 | https://graphika.com/reports/step-into-my-parler/ | accessed on 3 October 2020.
[3] Report | Graphika | "Operation Naval Gazing" | 22 September 2020 | https://graphika.com/reports/operation-naval-gazing/ | accessed on 23 September 2020.
[4] Report | Graphika | "Spamouflage Goes to America" | 12 August 2020 | https://graphika.com/reports/spamouflage-dragon-goes-to-america/ | accessed on 13 August 2020.
[5] Report | Graphika and DFRLab | "#OperationFFS: Fake Face Swarm" | 20 December 2019 | https://graphika.com/reports/operationffs-fake-face-swarm/ | accessed on 23 December 2019.
[6] News Article | Buzzfeed | "The Independent Used A Journalist Who Doesn't Exist On A Football Report from Cyprus." | 16 October 2017 | https://www.buzzfeed.com/markdistefano/the-independent-used-a-journalist-who-doesnt-exist-on-a | accessed on 17 February 2020.
[7] News Article | Reuters | "Deepfake used to attack activity couple shows new disinformation frontier" | 15 July 2020 | https://www.reuters.com/article/us-cyber-deepfake-activist/deepfake-used-to-attack-activist-couple-shows-new-disinformation-frontier-idUSKCN24G15E | accessed 17 February 2020.

TLP:WHITE

Victim Engagement IR Checklist

Management/General

Who is responsible for managing your networks?

- Are there multiple networks or system owners?

Have you hired or plan to hire a 3rd party remediator? If so:

- Who is the point of contact for the 3rd party remediator?
- Please consider authorizing the remediator to share data, including reports, raw data, malware and threat intelligence with the FBI.

Network Topology

How many networks exist and how are they connected?

Physical Network Topology

- Number of physical sites and how each site goes out to the Internet (direct Internet connections, backhaul via MPLS, etc.)
- Link type(s) (copper, single-mode/multimode fiber)
- Link speed(s) (1/10/40/100 gig)
- Peak/sustained network throughput for segments of interest

Logical Network Topology

- Outward facing IP addresses/Internet “points-of-presence”
- DMZ(s), their contents, and their IP ranges
- Proxy architecture and IP address(es)
- Load balancer(s) and IP address(es)
- List of all security appliances (NIDS/HIDS, firewall, antivirus, EDR - FireEye HX, Crowdstrike Falcon, Endgame, Tanium, etc.)
- Network segmentation (subnets/VLANS)
- DNS server configuration
  - Is DNS query logging enabled?

Which services (website, email, etc.) are hosted externally or in the “cloud”?

How is VPN/remote access configured for offsite employees and/or remote sites?

Cryptography/Key Management

- How are certificates managed?
- Do hosts employ full-disk encryption (Bitlocker, FileVault, etc.)?
    - Are recovery keys centrally managed?
- Where is SSL/TLS terminated (inbound/outbound)?

Authentication

- What centralized authentication is employed (Active Directory/LDAP)?
    - Determine Active Directory domain forests and cross domain trusts
    - Do Linux/Unix servers use centralized authentication?
    - Are there systems that don’t use centralized authentication?
    - Do VPN and/or cloud accounts use AD/LDAP or separate credentials?
    - Is two-factor authentication enabled for any services?
- How are privileged accounts managed?
    - Do administrators use these accounts for day-to-day work?
    - Multi-factor authentication?
    - How are these accounts monitored?
    - Are there local admin accounts (Windows/*nix)
- How are service accounts managed?
    - What privilege level do these accounts have?
    - Do these accounts allow interactive logon?

Monitoring/Security

- What kind of network data is routinely monitored/collected? (full PCAP, netflow, etc.)
- Are any network intrusion detection systems (IDS) in use?
- Are network taps in place or is there an ability to create SPAN ports for network monitoring?
- Is SSL/TLS breakout/inspection performed (inbound/outbound)?

Servers/Workstations/Other Devices

Total number of hosts in the environment

Operating systems/versions in use (Windows, Unix/Linux, Solaris, Mac OS, etc..)

- Number of each

Which servers are physical vs. virtual?

Virtualization platforms (VMWare, HyperV, etc..) in use?

What software packages are used in the enterprise?

- Are users allowed to install software?
- Is a “gold image” of the standard desktop install available?

- What is your bring-your-own-device (BYOD) policy, if any?

What antivirus and/or host intrusion detection software is in use?

Is there a centralized patch management/software deployment system in use?

Is there any endpoint detection and response (EDR) software in use?

Do you have the ability to collect forensic images of disks/memory?

Is there centralized log collection/storage?

Do you employ a security information and event management (SIEM) solution?

Consent/Legal

Who has authority to sign legal consent documents?

Is your organization willing and able to consent to a search of computer systems/networks by the FBI?

- Are there any restrictions on the scope of the consent?
- An FD-941 (“Consent to Search Computers”) agreement will need to be signed outlining the scope of the consent to search.

Is your organization willing and able to consent to network traffic monitoring?

- FD-1070 and FD-1071 will need to be signed for any network monitoring performed by or at the request of the FBI

Is your organization willing to allow the FBI to deploy distributed scanning or EDR tools to collect evidence?

- Signed consent for network investigative activity if endpoint agents (Endgame/Waldo) are going to be deployed

Are there policies in place to allow search and/or monitoring of business computers?

- How are these presented (logon banners/user agreements/manuals/training)?
- Copy of corporate IT policy and computer banner notifying users.

If possible, please provide copies of any relevant logs:

- Host systems (e.g., Active Directory logs, event logs, web server logs, etc.)
- Network Logs (e.g., IDS, firewall, VPN, DNS, web proxy, netflow, etc.)
- Other security appliances (e.g., EDR, SIEM, etc.)

Please provide any malware samples already discovered

- Please provide copies of any relevant phishing emails received with full headers

If incident response or investigation has already been conducted, either internally or by 3rd party IR providers please provide:

- Any finished or draft reports
- Any raw evidence collected, such as disk/memory images or PCAP data.

So You Reported. What Now?

- (U) The FBI has a myriad of tools to assist victims of cyber attacks and prevent future attacks from occurring.
- (U) Federal statutes, laws, policies, and directives put the FBI in a unique position to collect both: investigative information and intelligence regarding cyber matters.
- (U) The FBI works with the United States Intelligence Community (USIC), other Federal agencies, international partners and law enforcement, and United States local, tribal, and territorial law enforcement to identify emerging threats and determine tactics and techniques of cyber adversities.
- (U) Through investigations and intelligence collection, the FBI may be able to provide companies with information about who is targeting certain companies and sectors (Nation States versus Criminal Actors), the methodology behind actors' operations, attack patterns, and motives behind nefarious acts.
- (U) The FBI maintains excellent relationships with domestic and foreign law enforcement organizations and has access to tools that can assist victims in recovering losses, when possible, conduct cyber investigations domestically and abroad, and bring about convictions.
- (U) The FBI places a priority on conducting investigations that cause as little disruption as possible to a victim organization's operations. We recognize the need for cooperation and discretion, and, when necessary, will seek protective orders to protect business confidentiality.

(U) FBI Cyber Resources

(U) CyWatch

24/7 Operation

(855) 292-3937

cywatch@ic.fbi.gov

(U) Cyber Task Force

Located within 56 local FBI field offices

www.fbi.gov/contact-us/field

(U) Internet Crime Complaint Center

www.ic3.gov

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
INTEGRITY