To submit copies of this form via facsimile, please FAX to 202-406-9233.

Network Incident Report

United States Secret Service • Financial Crimes Division • Electronic Crimes Branch
Telephone: 202-406-5850 FAX: 202-406-9233 e-mail: ecb@secretservice.gov

Subject:
☐ Site under attack ☑ Incident investigation in progress ☐ Incident closed

What assistance do you require:
☐ Immediate call
☑ None needed at this time
☐ Follow-up on all affected sites
☐ Contact the "hacking" site(s)

Site involved *(name & acronym):*

POC for incident:
• Name / Title Austin Eversole
• Organization Drexel University
• E-mail myEmail@gmail.com • 7 x 24 contact information

Alternate POC for incident:
• Name / Title
• Organization
• E-mail • 7 x 24 contact information

Type of Incident:
☑ Malicious code: virus, Trojan horse, worm
☐ Probes/scans (non-malicious data gathering--recurring, massive, unusual)
☐ Attack (successful/unsuccessful intrusions including scanning with attack packets)
☐ Denial-of-service event
☐ High embarrassment factor
☐ Deemed significant by site

Date and time incident occurred *(specify time zone):* 1:57 PM PST 8/15/22

A summary of what happened:
Pegasus spyware installed on iPhone 12 and has likely been active for some time now

Type of service, information, or project compromised *(please provide specifics):*
☑ Sensitive unclassified such as privacy, proprietary, or source selection
Personal information information - Calls, SMSs, audio and video feeds from phone
☐ Other unclassified

Damage done:
• Numbers of systems affected 1
• Nature of loss, if any
• System downtime
• Cost of incident: ☑ unknown ☐ none ☐ <$10K ☐ $10K - $50K ☐ >$50K

Name other sites contacted
Law Enforcement Philadelphia Police Department
Other:

Details for Malicious Code

Apparent source:

- ❑ Diskette, CD, etc.
- ❑ E-mail attachment
- ☑ Software download

Primary system or network involved:

- IP addresses or sub-net addresses _____
- OS version(s) iOS 14.6
- NOS version(s) _____
- Other _____

Other affected systems or networks (IPs and OSs):

Type of malicious code *(include name if known):*

- ❑ Virus _____
- ☑ Trojan horse Pegasus Spyware for iOS
- ❑ Worm _____
- ❑ Joke program _____
- ❑ Other _____

- ❑ **Copy sent to**
- ☑ Amnesty International Tech
- ☑ Citizens Lab (University of Toronto)
- ❑ _____

Method of Operation *(for new malicious code):*

- ❑ Type: macro, boot, memory resident, polymorphic, self encrypting, stealth
- ☑ Payload
- ☑ Software infected
- ❑ Files erased, modified, deleted, encrypted *(any special significance to these files)*
- ❑ Self propagating via e-mail
- ❑ Detectable changes
- ❑ Other features

Details:

"bh" payload process remotely ran, after which spyware obtained root permissions on the iPhone and disabled Apple crash reporting software as well as installed its own surveillance software

How detected:

Ran Mobile Verification Toolkit (Amnesty International) and checked against Pegasus IOC's

Remediation *(what was done to return the system(s) to trusted operation):*

- ❑ Anti-virus product gotten, updated, or installed for automatic operation
- ❑ New policy instituted on attachments
- ❑ Firewall or routers or e-mail servers updated to detect and scan attachments

Details:

After backing up data victim wanted externally, reflashed iOS 14.6 to iPhone

Additional comments:

Details for Probes and Scans

Apparent source:

- IP address _____
- Host name _____
- Location of attacking host: _____
  - ❑ Domestic
  - ❑ Foreign
  - ❑ Insider

Primary system(s) / network(s) involved:

- IP addresses or sub-net addresses _____
- OS version(s) _____
- NOS version(s) _____

Other affected systems or networks (IPs and OSs):

Method of Operation:	**Details:**
❑ Ports probed/scanned ❑ Order of ports or IP addresses scanned ❑ Probing tool ❑ Anything that makes this probe unique	
How detected:	**Details:**
❑ Another site ❑ Incident response team ❑ Log files ❑ Packet sniffer ❑ Intrusion detection system ❑ Anomalous behavior ❑ User	

Log file excerpts:

Additional comments:

Details for Unauthorized Access

Apparent source:

- IP address: 217.70.184.38
- Host name: urlpush[.]net
- Location of attacking host: France
  - ☐ Domestic
  - ☑ Foreign
  - ☐ Insider

Primary system(s) involved:

- IP addresses or sub-net addresses:
- OS version(s): iOS 14.6
- NOS version(s):

Other affected systems or networks (IPs and OSs):

Avenue of attack:	**Details:**
☐ Sniffed/guessed/cracked password ☐ Trusted host access ☑ Vulnerability exploited ☑ Hacker tool used ☐ Utility or port targeted ☐ Social engineering	Used network injection to redirect user to malicious website, then used zero-click zero-day vulnerabilities to install a toolkit that gets root access and installs the surveillance payloads

Level of access gained-root/administrator, user

Root permissions are obtained by the 'bh' process

Method of operation of the attack (more *detailed description of what was done):*	**Details:**
☐ Port(s) or protocol(s) attacked ☑ Attack tool(s) used, if known ☑ Installed hacker tools such as rootkit, sniffers, 10phtcrack, zap ☑ Site(s) hacker used to download tools ☐ Where hacker tools were installed ☐ Established a service such as IRC ☐ Looked around at who is logged on ☑ Trojanned, listed, examined, deleted, modified, created, or copied files ☑ Left a backdoor ☐ Names of accounts created and passwords used ☑ Left unusual or unauthorized processes running ☐ Launched attacks on other systems or sites ☐ Other	Pegasus spyware was used to perform this attack. Within Pegasus is a toolkit likely named BridgeHead which runs as the process bh. This toolkit gains root access, disables apple crash reporting, and installs additional spyware onto the iPhone Website hacker redirected victim to in order to run exploit: https://gnyjv1xltx.info8fvhgl3.urlpush[.]net:30875/zrnv5revj Pegasus spyware examined almost all communications on the victims iPhone, and left backdoors for future access.

Details for Unauthorized Access (continued)

How detected:	Details:
❑ Another site ❑ Incident response team ☑ Log files ❑ Packet sniffer/intrusion detection software ❑ Intrusion detection software ❑ Anomalous behavior ❑ User ❑ Alarm tripped ❑ TCP Wrappers ❑ TRIPWIRED ☑ Other	The Mobile Verification Toolkit, especially made to detect Spyware like Pegasus, read analysis of records from iOS backups and filesystem dumps and logs and found Pegasus spyware IOCs on victims iPhone

Log file excerpts:

The malicious website containing the exploit used to deploy Pegasus spyware, urlpush[.]net, was found in the Twitter app's WebKit local storage, as well as IndexedDB folders on the iPhone.
This suggests that the victim opened the Twitter app and viewed a link within the Twitter app that opened up a local Safari page, which was redirected using network injection with a rouge cell tower or dedicated wireless equipment

Remediation *(what was done to return the system(s) to trusted operation):*	Details:
❑ Patches applied ❑ Scanners run ❑ Security software installed: ❑ Unneeded services and applications removed ☑ OS reloaded ❑ Restored from backup ❑ Application moved to another system ❑ Memory or disk space increased ❑ Moved behind a filtering router or firewall ❑ Hidden files detected and removed ❑ Trojan software detected and removed ❑ Left unchanged to monitor hacker ❑ Other	Because Pegasus likely doesn't run with full persistence anymore, reflashing the iOS on the iPhone should remove all traces of Pegasus spyware. Victim was notified of network injection attacks and how to best avoid them when being personally targeted

Additional comments:

Leaving the device unchanged to monitor the hacker was discussed, however Pegasus prevents other applications from jailbreaking the iPhone which could have been an ideal way to monitor the hacker. Additionally, the victim's "handler" using the Pegasus spyware may notice the lack of legitimate business communications from the victims phone and become suspicious

Details for Denial-of-Service Incident

Apparent source:

- IP address _____
- Location of host:
  - ❑ Domestic
  - ❑ Foreign
  - ❑ Insider

Primary system(s) involved:

- IP addresses or sub-net address _____
- OS version(s) _____
- NOS version(s) _____

Other affected systems or networks (IPs and OSs):

Method of Operation:	**Details:**
❑ Tool used ❑ Packet flood ❑ Malicious packet ❑ IP Spoofing ❑ Ports attacked ❑ Anything that makes this event unique	
Remediation ***(what was done to protect the system(s)):*** ❑ Application moved to another system ❑ Memory or disk space increased ❑ Shadow server installed ❑ Moved behind a filtering router or firewall ❑ Other	**Details:**

Log file excerpts:

Additional comments: