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)?

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?

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.

Operational Security/Other

Since there is a chance that email servers/accounts may be compromised, it is best to use out-of-band communications methods, such as an external email account, or telephone for all incident response coordination, including communication with the FBI.

It is your choice whether to upload any malware samples to services such as VirusTotal. In some cases, this may provide the threat actor an indication that their malware has been detected and possibly cause a shift in TTP's in response.

The FBI cannot provide remediation services nor recommend any private vendor of products or service, but the NSA Information Assurance Directorate maintains a list of Cyber Incident Response Accredited (CIRA) companies: https://apps.nsa.gov/iaarchive/library/supporting-documents/nscap-cira-accredited-companies.cfm

Notes:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____