Interested in learning more about security?

SANS Institute

Security Consensus Operational Readiness Evaluation

SCORE Security Checklist

The six step incident handling process is appropriate for all forms of incidents, including Advanced Persistent Threat (APT) style attackers. The APT is characteristically well funded teams of workers who are tasked with ex-filtrating intellectual property from targeted organizations. The data sought is typically insufficiently defended relative to its value, creating a situation where funding the theft of the data is economically advantageous compared to developing the data from scratch. At times, however, the adversary's intent is to diminish the value of the data to the rightful owner. Denial of service reduces the availability of the data. Potentially more damaging would be manipulating the integrity of the data such that the data owner acts in error based on the tampered data.

While the Incident Handling process is adaptable to respond to APT style attacks, and some actions should be taken for any incident regardless of the threat involved, there are response strategies that are better suited to an APT compromise. The following outline is intended to be a checklist of actions appropriate to dealing with the threat and a compromise accomplished by this threat. Customized tailoring to each environment and situation is warranted and recommended. But this guide is a generalized set of actions appropriate to APT response.

1. Preparation
    1. Identify ownership and responsibility for all systems (including data) in the enterprise
    2. Clear communication channels
        1. Capabilities for encrypted email communication (potentially not using primary email server)
        2. Capabilities for encrypted chat messaging (potentially not using primary chat server)
        3. Telephone call list for coordination stored offline
        4. Understanding which parties are to be notified
            1. Develop contact list per system
                1. System Owner
                    1. Possibly designated Point of Contact (POC), too
                2. Technical POCs
                    1. Possible after hours / rotation / call list for response
    3. Incident Response aware of and capable to address APT style attacks
        1. Clear understanding of this threat's characteristics
            1. Management has clear understanding of the threat
        2. Authorized to respond on all systems in enterprise
        3. Funded to perform extended investigations
            1. If Incident handling isn't currently 24x7, what resources are available to continue IR work throughout sustained response
    4. In house capability or contracts with business partner for
        1. Incident Response
        2. Forensic Investigation
        3. Malware Reverse engineering
    5. Containment Strategy for APT
        1. Two basic strategies:
            1. Watch and Learn
            2. Disconnect
        2. Define the Standard Operating Procedures (SOP) for when each scenario is used
        3. Define a methodology for an incident responder to deviate from SOP as needed

        1. This methodology should be part of SOP
            1. Include steps for notification and justification of planned deviation
    6. Press Team
    7. Legal Team
2. Identification
    1. Remote Access Trojan (RAT)
    2. Command and Control (C+C)
    3. Encrypted Communications discovered
    4. Covert Channel discovered
    5. Host based IDS/IPS alert of unexpected system call, data access, port open
    6. Direct External Notification (Law Enforcement, Business Partner)
    7. Indirect External Notification (Open Source Intelligence of behavior, search in your environment)
    8. Data discovered outside of organization (pastebin, news)
    9. Blackmail “offer”
    10. Notification to internal staff must occur in a discrete fashion
        1. Encrypted
        2. Limited to only those with need to know
        3. Authorization to add additional resources to response effort is limited to Incident Response Management, and/or Business Unit Management
        4. Categorize known Severity and Impact
        5. Provide updates as important new information comes to light
3. Containment
    1. Watch and Learn versus Disconnect
        1. Have this plan in place in advance! (per Preparation phase)
    2. Extract and identify characteristics of adversary
        1. Identify other affected systems
        2. Utilize updated Network Intrusion Detection System (NIDS) / Network Intrusion Prevention System (NIPS) / Host Intrusion Detection System HIDS / Host Intrusion Prevention System (HIPS) signatures to assess assets throughout environment.
            1. Update NIDS/NIPS/HIDS/HIPS to search for characteristic:
                1. Files
                2. System calls
                3. Processes
                4. Network
                    1. Ports
                    2. IP addresses
                    3. Host names
            2. Use Packet Capture (pcap) / network forensic devices to replay old traffic to identify additional infected systems
    3. Identify what has been stolen
        1. Full pcap (which retains a copy of all data from the wire) is invaluable in this regard
            1. Even w/ full pcap, traffic may be encrypted
            2. Must break encryption to fully assess damage
            3. May need host based forensics in coordination with full pcap to complete this assessment
        2. Intellectual Property

3. Resources
    1. Bandwidth
4. Identify legal ramifications
    1. PCI
    2. HIPAA
    3. California HR (SB 1386) notification requirements
    4. European data breach requirements
    5. Many possible other legal ramifications
5. Is it appropriate to remove entire segment from network (disconnect?)
    1. May be easier to identify malicious network traffic if the environment is still online because the traffic is still flowing, but may have ongoing loss of data
6. Contact Law Enforcement (LE)?
    1. FBI typically interested in this sort of attack
    2. The decision to involve LE may affect the amount of and degree of public reporting
7. Public Reporting?
    1. US-CERT
    2. Industry requirements?
        1. Defense Industrial Base (DIB)
        2. Medical
        3. Sarbanes-Oxley (SOX) / Gramm-Leach-Bliley (GLB)
    3. Partner notification
    4. Customer Notification

4. Eradication
    1. Imperative that all affected systems be collected, and full forensic images be made.
        1. Memory Images very important for APT since some techniques do not write to hard drive
            1. Also may assist in assessment of ex-filtrated data
                1. If data ex-filtration uses symmetric cipher, then decryption key will be present in Random Access Memory (RAM)
        2. Preferred method is to seize hard drives as evidence, replace those hard drives with new system image.
            1. Preferred because this drive is the legal evidence of wrongdoing
            2. Any pcap / network information that could be evidence must also be preserved
                1. Have SOP showing handling of evidence for pcap
                2. Associate with case, make MD5 and SHA256 hash of stored pcap
        3. Secondary option is to make forensic image (for example, remotely via encase enterprise or another enterprise forensic solution, then wipe drives and re-image
        4. Without this evidence, a thorough investigation cannot be completed
    2. Close all network vectors of ex-filtration
        1. HTTPS inspection via proxy and Secure Socket Layer (SSL) intercept
        2. Prohibit outbound encrypted communication except for known, authorized peers
        3. Techniques demonstrated during this APT incursion
    3. Close all vectors of re-infection
    4. Remove all RAT / C+C / Backdoors
5. Recovery
    1. Close future network vectors of ex-filtration
        1. HTTPS inspection via proxy and SSL intercept

    2. Prohibit outbound encrypted communication except for known, authorized peers
2. Re-engineer systems to prevent reinfection
3. Segment critical data to more restricted areas
4. Implement auditing for critical data access
5. Identify individuals within environment who purposefully or accidentally aided APT, for counseling / training / discipline

6. Lessons Learned
    1. Assess Executive posture toward Incident Handling and Information Assurance. Is this loss just a cost of doing business, or is it an opportunity for massive change?
    2. Develop Intelligence group for identification of APT attacks
        1. Characterize the adversary
            1. Use “Kill Chain” model or other counter-intelligence strategies
            2. Adversary has limited resources, as well. Will re-use assets.
            3. Attribution is very difficult, but is the end goal for counter-intelligence activities.
    3. Campaign to assist business members of various sorts of threats
        1. Malware drive by download = smash and grab from car
        2. APT = home invasion / hostage situation
        3. Explain potential loss of long term competitive advantage of business due to loss of IP
    4. Re-catalog and re-value assets in light of APT strategies and targets
        1. Avoid Blame, use incident to enhance capabilities
    5. Enhance methods for APT response, including
        1. “Watch and learn” capabilities
        2. Honey tokens for Intellectual Property (IP)
        3. Active honey-nets
        4. Deception capabilities
    6. Aggregation of data from all sources
        1. Security Information and Event Management (SIEM) if possible
        2. Identify additional data sources
            1. Firewalls
            2. HIDS
            3. Windows Active Directory (AD) / Lightweight Directory Access Protocol (LDAP) / Authentication
            4. Wireless infrastructure
            5. Any system not currently providing data
                1. Servers
                    1. Web servers
                    2. Data base servers
                2. Workstations
                3. Mobile devices

Last Updated: November 5th, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS San Diego Fall 2018	San Diego, CAUS	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS Mumbai 2018	Mumbai, IN	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS Rome 2018	Rome, IT	Nov 12, 2018 - Nov 17, 2018	Live Event
Pen Test HackFest Summit & Training 2018	Bethesda, MDUS	Nov 12, 2018 - Nov 19, 2018	Live Event
SANS November Singapore 2018	Singapore, SG	Nov 19, 2018 - Nov 24, 2018	Live Event
SANS ICS410 Perth 2018	Perth, AU	Nov 19, 2018 - Nov 23, 2018	Live Event
SANS Paris November 2018	Paris, FR	Nov 19, 2018 - Nov 24, 2018	Live Event
SANS Austin 2018	Austin, TXUS	Nov 26, 2018 - Dec 01, 2018	Live Event
European Security Awareness Summit 2018	London, GB	Nov 26, 2018 - Nov 29, 2018	Live Event
SANS San Francisco Fall 2018	San Francisco, CAUS	Nov 26, 2018 - Dec 01, 2018	Live Event
SANS Stockholm 2018	Stockholm, SE	Nov 26, 2018 - Dec 01, 2018	Live Event
SANS Khobar 2018	Khobar, SA	Dec 01, 2018 - Dec 06, 2018	Live Event
SANS Nashville 2018	Nashville, TNUS	Dec 03, 2018 - Dec 08, 2018	Live Event
SANS Dublin 2018	Dublin, IE	Dec 03, 2018 - Dec 08, 2018	Live Event
SANS Santa Monica 2018	Santa Monica, CAUS	Dec 03, 2018 - Dec 08, 2018	Live Event
Tactical Detection & Data Analytics Summit & Training 2018	Scottsdale, AZUS	Dec 04, 2018 - Dec 11, 2018	Live Event
SANS Frankfurt 2018	Frankfurt, DE	Dec 10, 2018 - Dec 15, 2018	Live Event
SANS Cyber Defense Initiative 2018	Washington, DCUS	Dec 11, 2018 - Dec 18, 2018	Live Event
SANS Bangalore January 2019	Bangalore, IN	Jan 07, 2019 - Jan 19, 2019	Live Event
SANS Sonoma 2019	Santa Rosa, CAUS	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Amsterdam January 2019	Amsterdam, NL	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Threat Hunting London 2019	London, GB	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Miami 2019	Miami, FLUS	Jan 21, 2019 - Jan 26, 2019	Live Event
Cyber Threat Intelligence Summit & Training 2019	Arlington, VAUS	Jan 21, 2019 - Jan 28, 2019	Live Event
SANS Dubai January 2019	Dubai, AE	Jan 26, 2019 - Jan 31, 2019	Live Event
SANS Las Vegas 2019	Las Vegas, NVUS	Jan 28, 2019 - Feb 02, 2019	Live Event
SANS Security East 2019	New Orleans, LAUS	Feb 02, 2019 - Feb 09, 2019	Live Event
SANS Osaka 2018	OnlineJP	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced