TEAMT5

Incident Response

In order to expand the business and the collaboration with customers, enterprises and organizations have extensive use of network to provide services. However, hackers may exploit the network access to initiate attacks, causing operation shutdown and damaging brand value and customer rights. The incident response aims to reduce the losses caused by attacks and help the organization recover as soon as possible.

TeamT5 Incident Response Services - Professional Analysis, Investigation, Response

TeamT5, which has been researching global threat intelligence and tracking malicious programs for a long time, is well aware of the emergency response needs of organizations facing cybersecurity attacks, and provides professional Incident Response (IR) services to help organizations quickly and effectively handling cyber incidents, protecting critical digital assets, shortening the suspension time of network services, and ensure that operation resumes and runs normally.

By deploying the ThreatSonar Threat Forensic Analysis Platform developed by TeamT5, users can quickly detect threats and risks in the environment, starting the investigation from the hosts that were severely compromised to the overall security status of endpoints. At the same time, by analyzing key network logs, we clarify the possible access points of hackers and root causes, identify the lateral movement, and evaluate the threat damages. We furtherly provide suggestions on how to improve the security measures and defense similar attacks in the future.

Preparation

- Clarify incident status
- Identify customers' requirement
- Emergency containment suggestions
- Provide IR plan

Detection

- Endpoint scan (ThreatSonar)
- Collect and analyze critical evidences
- Identify the compromise scope

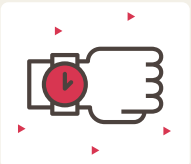
Investigation and Response

- Sample analysis
- Log analysis
- Threat hunting
- Identify root cause
- Containment recommendations

Enhancement Suggestions

- Incident report with interpretation by dedicated personnel
- Threat intelligence feedback for real-time defense and block
- Root cause analysis and cybersecurity improvement recommendations

Benefits



❶ Block threats and grasp the critical time to collect evidence

- Provide response suggestions immediately and collect criticle evidence for incident retrospective.
- Deploy ThreatSonar to quick scan threats in the environment.

❷ Comprehensively investigate suspicious threats to eliminate further attacks

- When starting the investigation of main hacked hosts, the compromise scope will be also identified.
- Perform correlation investigation to find out whether there is any lateral movement.

❸ Professional and precise incident analysis to minimize damage

- Offer containment suggestions based on our research of adversary groups and TTP.
- Recovery suggestions with proficient in handing in C2, stolen credentials and other types of attacks.

❹ Detailed incident investigation and prevention suggestions

- IR experts conduct and present complete incident reports, incuding root cause analysis and improvement suggestions.
- Combine relevent intelligence and incident analysis to strengthen organizations' proactive defense.

Industry and Customer Recognition

Offline, onsite, or remote investigations

- Preserve and analyze the log data and file system.
- Identify the root cause of the incident, compromised hosts and provide the mitigation suggestions.

System/Web/AP log analysis

- Find out the source of attacks and attack patterns.

Malware analysis

- Sandbox and professional manual analysis on provided malware sample.

Experiences in handling various types of cyber incidents

- Ransomware
- APT attacks
- SQL injection
- Website hacking
- VPN credentials leak
- Data breaches
- Phishing
- Compromised devices

Expertise in Incedent Reponse

More than 20 years of experience in reserach-ing in malware and APT with pratical experience in handling incidents.

Industry-leading Adversary Research

We specialize in adver-sary analysis, threat hunting, vulnerability research, and root cause analysis.

Certified IR Profession

Obtained professional certificates, including ECSA, CISSP, CEH, CHFI, etc.

Lecturer-level IR Expert

Participated in and gave speeches at internation-al professional cyberse-curity seminars, such as Black Hat (US), JSAC (Japan), CodeBlue (Ja-pan), etc.

World-class Industry Network

TeamT5 CSIRT is a mem-ber of FIRST, the world's largest incident respon-se organization.

Widely trusted by more than 300 customers around the world, including government departments, technology, manufacturing, finance, medical care, military, telecommunications and other industries.

ThreatSonar

Threat Forensic Analysis Platform

Quick Scan, Efficient Incident Investigation

Detected
1,000+
APT attacks that other cybersecurity solutions couldn' t find

Over
90%
managed security services providers in Taiwan adopted

Implemented
3 million+
endpoints forensics

Industry-leading Features

Lightweight deployment and background execution without affecting daily operations

ThreatSonar agent can be deployed on thousands of computers, and runs with less system resources. Personnel can carry out computer work as usual without the burden of running scans.

Possess memory forensics and behavior analysis to effectively identify unknown malicious programs

Identify malicious programs hidden in the memory, executed and to-be-executed programs, attacker's hacktools, artifacts left on the host, and hundreds of dynamic behavior anomalies.

Active threat hunting with visualization of correlating potential compromised endpoints

Statistical correlation analysis finds unknown attack techniques, establishes baselines to lock on abnormal behaviors, and tags poten-tial unknown threats.

TeamT5 | Tel 02-7706-1299 | E-mail sales@teamt5.org