Malware & Advanced Persistent Threat (APT) Remediation Services

EMAGINED SECURITY®

Overview

Malware/APT Remediation Services supports the eradication of Virus/Worm/Trojan or other types of Malware/APTs that can be present on computer systems that have been infected. Emagined Security provides off-site and on-site resources (as required) to identify and investigate any indications of compromise to systems. Emagined Security uses a six phase approach to ensure that systems are remediated, clean and free of infections.

- Phase 1: Identify – Malware/APT Identification
- Phase 2: Triage – Containment
- Phase 3: Remediate – Malware/APT Removal
- Phase 4: Assess Residual – Identify Remaining Threats & Vulnerabilities
- Phase 5: Enhance Protection – Remediate Residual Threats & Vulnerabilities
- Phase 6: Maintain – Prevent Re-Occurrence

Benefits

Emagined Security has successfully guided Organizations & Users through Malware/APT data losses, breaches, and service interruptions. Based on our experience Emagined Security has developed this methodology to guide future clients through similar challenges. Emagined Security's has created a six phased methodology to effectively regain control and mitigate risks.

Recognizing what has led to a security Malware/APT identification is crucial to minimizing the potential of future occurrences. Whether initiated by spam & websites, Phishing, disgruntled employee, malicious competitor, misguided hacker, or deliberate attacks; Virus/Worm/Trojan/APT compromise often cause damage and disruption equal to or greater than any natural disaster.

Emagined Security provides Malware/APT remediation services tailored to your needs. We provide these services to customers in the following ways:

- Level 1 – On Demand Support (Phone/Remote Access)
- Level 2 – On Demand Incident Response (Phone/Remote Access/On-site)
- Level 3 – On Call Corporate Retainer (Phone/Remote Access/On-site)
- Level 4 – On Call Corporate Retainer For Company and Customers (Phone/Remote Access/On-site)

Description of Service

Emagined Security supplies technical, investigative, and advisory forensics support relating to Malware/APT event. In addition, Emagined Security can perform analysis/interpretation of data, discovery and handling of evidence, documentation of efforts, procedural recommendations, technical advice, and related investigations. With respect to a Malware/APT compromise, Emagined Security typically performs the following tasks:

Phase 1: Identify – Malware/ATP Identification

The first phase begins with identifying if a compromise has been realized. A variety of tools and analysis techniques can be used to determine if issues exist on your network. The following is a list of some tools and techniques that may be employed:

- Anomalous Traffic Identification
  - Internal servers suddenly initiating connections to the Internet when this is not part of normal operations. (e.g., NetWitness)
  - Systems connecting to known bot, bad actor, or C&C hosts on the Internet (e.g., Symantec Web Gateway)
  - Odd encapsulation of traffic or unexplained encrypted tunnels (e.g. ssh tunneling through https or data embedded into ICMP)
- Identification of Gaps in System and Security Logs
- Review of Unexplained Changes in System Configurations
- Intrusion Detection Systems
- Multi-vector APT Threat Intelligence (e.g., FireEye)
- Anti-Virus Systems
- Network Sniffers

Many of these tools may already be owned by your organization or can be licenses or purchased to support the investigation, as needed.

Phase 2: Triage – Containment

The Triage Security phase typically begins with a discovery session where the appropriate parties from within the pertinent areas of your Organization/Users are formally identified and a formal project is initiated by this Triage Team. The Triage Team works closely with the Incident Response Team and End Users to assess the compromise level.

The primary goal of the Triage Team is to analyze the information available at hand to "contain malicious behavior". This involves reviewing the Malware/APT payload, identify and analyze the effects of the Malware/APT, stop the spreading and determine appropriate remediation action to remove the Malware/APT from the Organization/User Systems.

The Triage phase ends once Team Members are confident that the identified Malware/APT has stopped spreading and the compromise is understood.

Phase 3: Remediate – Malware/APT Removal

Emagined Security next determine what the Malware/APT is doing forensically, validate if the Trojan is trying to communicate externally and determine what, if any disclosures may have taken place. If communication channels have been opened, Emagined Security will identify communication channels and determine appropriate steps are required to block the Malware/APT from communications at the firewall or on the infected system.

Emagined Security reviews the current remediation steps identified by Antivirus companies instructions and determines if an automated approach for removal of the Malware/APT is available while validating that the steps are appropriate based on identification of Malware/APT activity. Emagined Security adds any steps not identified in current remediation steps to ensure comprehensive removal of the Malware/APT.

If needed for organization, Emagined Security will define or create a remediation script if possible and not currently available. This script can be used by organizations to remediate the compromise on several systems in a more automated fashion to remove the Malware/APT from company systems.

Phase 4: Assess Residual – Identify Residual Threats & Vulnerabilities

Upon completion of removal of the identified Malware/APT, Emagined Security begins an effort to ensure that any compromise root causes are identified. This includes a review of the organization's/user's security protection in the perimeter, host, and other endpoint environments. By using root causes and infrastructure reviews, Emagined Security creates a list of additional steps that may be undertaken by the Organization/User or contracted to Emagined Security to help address.

Phase 5: Enhance Protection – Remediate Residual Threats & Vulnerabilities

Upon identification of root causes and completion of the infrastructure review, Emagined Security will create a recommendation to ensure that future infections protections are in place. Emagined Security typically makes recommendations of solutions/products that can be used to address these issues identified during this process.

Phase 6: Maintain – Prevent Re-Occurrence

Once remediation efforts are completed, it is necessary to maintain the improved control environment to prevent re-occurrence of issues. If desired, Emagined Security can be contracted to perform these additional tasks. Tasks typically include Malware/APT protection installation, maintenance and tuning along with a variety of various security enhancement services.