GIAC Enterprises

Security Controls Implementation Plan

Group Discussion and Written Project

John Hally, Erik Couture
08/07/2011

Table of Contents

Executive Summary

The cyber-threat landscape has evolved significantly in recent years. From primarily a threat of denial of service and website vandalism in years past, to the currently advanced and well resourced adversaries employing complex technologies to achieve financial and political benefit. At GIAC Enterprises, we have observed huge increases in suspicious network activity directed at our corporate networks, sometimes even targeting key individuals. Due to the huge global increase in demand for fortune cookie messages, it is reasonable to expect that this undesired attention will only increase in the coming months and years as cyber-criminals and possibly corporate spies attempt to closely monitor our business activities and steal vital business information.

This paper presents the recommendations of the tiger team, which was recently formed, with the goals of:

1. Developing a strategy for the implementation of the SANS Top 20 Security Controls, and in particular the creation of an incident response capability; and
2. Identifying and eradicating any possible current malware infections.

We strongly recommend a focus on detection; the computer security adage goes: "Prevention is ideal, but Detection is a must". We recommend the implementation of a phased implementation of the SANS Top 20 Controls over the next several months; first focusing on identifying and removing any existing malware, followed by the implementation of a robust incident handling process which will aim to detect and mitigate any future threats. This incident response capability will help allow time for additional security controls to be brought on line in a logical order to maximize their positive impact on the security of our networks and by extension, the profitability and continued success of GIAC Enterprises business.

Introduction

This tiger team was initiated partially in response to a briefing given to management from an outside security firm, outlining the possible threat of Advanced Persistent Threat (APT) malware; in particular the *Shady RAT*, a remote access tool or 'trojan' which has been deployed extensively and in a very targeted manner by elements of the APT.

The scope of this paper extends not only to addressing our exposure, if any, to this specific threat but presents a high-level plan for the implementation of computer security best-practices throughout our enterprise. The selected set of best-practices are the "SANS Twenty Critical Security Controls for Effective Cyber Defense" which form an excellent guide for the securing of any computer network, providing general guidance and suggested quick-action/high-payoff items to mitigate some of the most critical vulnerabilities as rapidly as possible.

This paper will first introduce the SANS 20 Security Controls and lay out a plan for their implementation, as appropriate. It will recommend a way forward in the creation of an incident response capability, including required procedural, technical and policy changes.

Finally, it will outline a deliberate network analysis and incident handling process with the goal of detecting any existing breaches (but focused on *Shady RAT* in particular) to the corporate network and remedying the situation as required.

Security Controls Implementation Plan

Computer security cannot be effectively addressed in a arbitrary manner. Rather, any effective long term defense must employ a well planned approach which considers the problem holistically; applying the principles of defense in depth, leveraging automation where possible, identifying and addressing the root causes of issues and providing measurable metrics of the effectiveness of the risk mitigation. It is in this spirit that the SANS 20 Critical Security Controls were developed as a framework to help guide organizations. The 20 Controls guidelines can appear somewhat overwhelming at first glance, as they seem to imply there are thousands of things to do, and most of it as a high priority. Clarity comes from the careful assessment of our organization's risk profile and current in-place policies. We can then achieve measured, incremental improvements step by step.

The first step is to undertake a gap assessment to determine our current security posture and risk profile. We will identify our most critical business information and map out where it resides, how it moves over the network, and who should have access to it. This will provide a baseline with which to identify the most critical security controls to implement. While the gap assessment has not yet been completed fully, a first draft of an order of priority is included in the Project Plan annex.

Once the critical gaps in our security posture have been identified and priority has been assigned to the security controls we wish to implement the implementation of Quick Win controls will provide a rapid benefit in key area, picking the proverbial low-hanging fruit and significantly reducing our risk profile; in many cases for very little cost. Several of the security controls should be work on concurrently; each will be assigned to a relevant departmental lead, such that System Administrators, Security Administrators, and management can collaborate and move ahead on a number of initiatives concurrently.

Security awareness and training, not just of technical staff but of all users, will pay dividends in faster identification of warning signs of possible network breaches. It will help reduce the danger of accidental or negligent internal threats and promote responsible and secure use of our corporate data and IT infrastructure. This training should be espoused at the highest level of management and afforded time and support to revisit on a regular basis.

Over time, as the initial controls are implemented, successfully automated and regularly audited, we should move to implement lower priority but still important control over the next 12-24 months.

Creating an incident response capability

The 18th Security Control involves the creation of an incident response (IR) capability. This capability is composed of much more then a group of individuals, which will respond to an incident. Such an incident handling (IH) team is certainly a key component of such a capability, but needs to be supported with a robust set of policies and processes to enable its success. Several of these supporting items are clearly outlined as Quick Wins (QWs) within the SANS Top 20. In the near term, GIAC Enterprises will implement the base of a holistic IR capability, whose first order of business will be to collaborate on a deliberate audit of our networks (described later in this document). The team will be comprised of:

- Team Lead - a member of senior management
- Technical Lead - CIO
- Senior Security Administrator
- Senior Network Administrator

This team will implement the following actions, as indicated on the timeline in the enclosed annex.

- Led by the Team Lead, the team will define and assign specific roles and responsibilities to the team members. Job titles and specific duties will be outlined, and alternative/backup members will be identified.
- Led by the CIO, the team will develop a clear IH process that will, in particular, define the critical points at which input and decisions are required. Details of the process are outlined in the following section.
- Led by the Senior Security Admin, a concise awareness document will be developed, targeted at the user base at large. The 'cheat-sheet' will educate the reader on what types of indicators of possible security issues to look for on the network, and when and how to report them. This document will be launched at an employee training session and will be revisited periodically.
- Led by the Senior Network Administrator, incident recovery standards will be developed and published. A thorough analysis of the networks, data centers and hosts will be conducted and estimates will be published indicated estimated time to repair and priority of repair. This document will form the basis for the response to any incident and will allow the IH team to rapidly allocate resources to recovering the most critical systems first.

The members of the IH Team must be carefully selected to possess the skills required for their effective leadership in preparation for, during and after a computer incident occurs. In particular, they must possess superior management skills, which will permit them to rapidly assess the situation and take sound action to minimize negative impacts. They must also possess strong technical and communications skills which will enable them to grasp the impact of the issue and concisely explain it to decision makers at relevant points in the incident response process.

The incident response capability should be exercised regularly to ensure all concerned individuals and decision makers are aware of their parts. The IR Weekend, described in this document, will provide our IH team an opportunity to exercise the foundations of our IR plan, noting lessons learned and improving the process for future iterations.

Incident Response Weekend Plan

A key assigned task of this tiger team is to develop a plan for the deliberate assessment of any current breaches of the network and conduct a thorough recovery over a planned weekend maintenance period. In particular, the tiger team has been assigned to assess the possibility of any breach by the *Shady RAT* malware. This strategy will involved significant pre-planning and coordination between all relevant parties and will be led by the IH Team as outlined above. In keeping with industry best practices, the six phases of incident response will be used as the basis for the incident response weekend plan. These phases are:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

Preparation

The preparation phase for the incident response weekend plan will consist of the following:

- Form IH team
- Create reporting structure
- Create communication plan

In close collaboration with the Detection tiger team, the IH team will leverage several tools and techniques for identifying advanced persistent threat (APT) behavior to seek out and eradicate *Shady RAT*, and any other infestations.

Creating a clear reporting structure within IH team and between system owners and management is critical for the success of the response plan. The IH team will need to know who to contact should any issues arise with the plan execution. System owners and management will need to be kept up to date with regard to systems that have been identified as compromised to determine the impact and risk to the organization due to the remediation process.

A communication plan will be created consisting of:

- Contact lists of key individuals from the reporting structure
- Phone bridge number(s)
- Fax numbers or other emergency methods of communication
- Email addresses and public encryption keys for encrypted communication

This communications plan will be exercised during the incident response weekend activities.

Identification

Identification of *Shady RAT* compromised systems will leverage the existing work of the Detection tiger team's implementation of correlation tools and network monitoring infrastructure. Because of the potential of the malware morphing as a result of direct attempts of identification (scanning, local system command execution, etc.), the identification process will be primarily passive in nature using network monitoring as the basis for detection. The identification process with consist of:

- Identify/implement new traffic signatures for Snort/Sguil detection (Emerging Threats)
- Identify infected systems based on IDS alerts, DNS queries, and correlation using the Security Onion installation. The following will be recorded for use during the containment and eradication phases of the response plan:
    - IP address

    - MAC address
    - Switch port locations (IP to MAC to CAM table associations)
    - Wireless access point associations if applicable.

Systems that have been identified will be evaluated based on business and asset criticality, and prioritized for the remaining incident response phases. System owners and management will be contacted to communicate the impact of containment and eradication phases on systems and gain authorization for remediation of critical systems. In the absence of any clear asset criticality identification, the following ratings will be used:

- Data center servers providing business functionality - High
- High level executives/technologists/support personnel desktops/laptops/tablets - Medium
- End user desktops/laptops - Low

Additionally, after consulting with forensics expert Rob Lee, the following additional steps should be taken in order to root out all malware infestations to have the best chance of eliminating the advanced persistent threat and mitigate reinfection from occurring:

- Live-image known systems that appear to be compromised.
- Complete a thorough forensic analysis of each image
- Use the information gleaned from the forensic analysis to develop additional detection mechanisms such as file hashes, registry keys and other malware threat intelligence.
- Process lists that have been statistically analyzed for 'Frequency of Least Occurrence'.
- Use this information to actively scan the enterprise looking for additional systems that are infected but lay dormant.

Using this approach iteratively to identify all infected systems, both active and dormant, will substantially increase the chances of successful elimination of the advanced persistent threat posed by malware used in Operation *Shady RAT*.

Containment

Once the compromised systems have been identified using the Detection tiger team's network detection and correlation tools, methodologies, and countermeasures, the containment phase of the incident response plan will be initiated. The containment phase will consist of the following tasks:

- Backup/forensic image of systems for post remediation analysis
- Shut down switch port and/or remove network cable of the compromised hosts
- Add MAC filters to wireless access points for any identified compromised wireless clients, disable wireless cards.
- Apply firewall rules for identified malicious ingress/egress traffic.
- Enable Intrusion Prevention System functionality.
- Force web traffic through proxies allowing only HTTP/HTTPS traffic to/from the proxy addresses at the firewalls.
- Leverage access controls and other security functionality within the proxy to mitigate attack vectors
- Implement file attachment scanning and/or stripping at the mail servers where applicable to mitigate the malicious file attachment attack vectors.

Close communication with the Detection tiger team during the containment phase will allow the IH team to determine containment progress based on alert generation or lack thereof. Additional anomalous behavior that is detected during this phase could indicate morphed malware that can be further analyzed and used for additional detection capabilities. Once alerts are no longer being generated for *Shady RAT* activity and a steady state has been reached, the eradication phase will begin. Additionally, system owners and management will be apprised of the execution and progress during this phase.

Eradication

Based on current research and analysis available, there is no current way to thoroughly clean a compromised system and be completely certain of the system's integrity. As such, the eradication phase requires a full disk wipe and re-image of the system. The following steps will be conducted to eradicate *Shady RAT* infections:

- Wipe system drive(s)
- Re-image systems/restore from backups
- Patch/harden Systems
- Install Anti-Virus, Anti-Malware, Host Intrusion Detection System (HIDS)

Care must be taken when re-imaging and/or restoring systems from existing system images and backups. If the integrity of the backups or system images is in question, a full re-installation of the systems and applications from original media may be necessary.

It is also important to fully patch and harden the operating systems as well as install enterprise Anti-Virus and Anti-Malware packages to help mitigate future compromise. Current analysis by Symantec has indicated that their anti-virus solution provides protection within their Trojan.Downbot family signatures against common threat vectors used by *Shady RAT* during the initial exploitation phase. Additionally, Symantec's reputation based technologies can also be leveraged to proactively protect systems against the common files used in these attacks

Host Intrusion Detection Systems such as OSSEC will also be installed to detect and correlate potential attacks and identify attack vectors for increased incident response capabilities in the future.

Recovery

Once the eradication phase has been completed, the recovery phase will be initiated. This phase returns the once-compromised systems back to their normal state and function. The recovery phase will consist of the following:

- Validate systems function normally
- Restore operations/accessibility to systems
- Monitor systems using:
    - Network IDS
    - Host-based IDS
    - System log monitoring

Monitoring of remediated systems during this phase is critical to determining if the incident has been completely mitigated or if there are still undiscovered attack vectors that allow for system compromise. Baselines should be taken and any anomalous traffic should be fully investigated in order to identify if additional remediation is required.

Lessons Learned

The final phase of the incident response plan will be to hold a Lessons Learned meeting with the IH and Detection tiger team. During this meeting any insights gained during the incident response plan execution can be distributed through the team members in order to increase the incident response capabilities of the team. The information and insights from these meetings will be used to initiate improvements to technology, processes and the incident handling capabilities of the response teams.

A final formal report of all weekend incident response activities will be created and distributed to system owners and management for review.

Conclusions

This report makes the following recommendations:

1. An incident handling team should be created and enabled with the time and resources to develop and implement a robust IH plan.
2. A planned outage should be conducted on an upcoming weekend in order to assess any possible exposure to threats and remedy as necessary. Significant time and resources will be required in the following days, prior to the planned outage to allow network security staff to conduct thorough passive analysis of the network traffic and develop the details of the weekend incident response plan.
3. In the medium and long term, GIAC Enterprises should dedicate the time and resources to implementing the SANS Top 20 Controls, in a measured and deliberate fashion, focusing on the implementation of Quick Wins to maximize the return on investment.

References

Revealed: Operation Shady RAT, Dmitri Alperovitch, Vice President, Threat Research, McAfee http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG), Version 3.0 April 15, 2011, http://www.sans.org/critical-security-controls/

Shady RAT Backgrounder: http://www.symantec.com/connect/blogs/truth-behind-shady-rat

Shady RAT Code: http://read.pudn.com/downloads119/sourcecode/windows/network/508294/htran/htran.cpp__.htm

Snort Signatures for Shady RAT behavior: Daily Update August 4th 2011, Signatures:2013361 2013362, 2803355, 2803356: http://blog.emergingthreatspro.com/2011/08/daily-update-summary-842011.html

Sourcefire Vulnerability Research Team: http://www.sourcefire.com/security-technologies/snort/vulnerability-research-team/advisories

Security Onion IDS: http://securityonion.blogspot.com/

Windows Incident Response, APT and Frequency of Least Occurrence: http://windowsir.blogspot.com/2010/01/thoughts-on-apt.html

NIST Special Publication 800-61: http://csrc.nist.gov/publications/nistpubs/800-61- rev1/SP800-61rev1.pdf