Joint Security Awareness Report

JSAR-12-241-01B—Shamoon/DistTrack Malware

UPDATE B

October 16, 2012

OVERVIEW

W32.DistTrack, also known as "Shamoon," is an information-stealing malware that also includes a destructive module. Shamoon renders infected systems useless by overwriting the Master Boot Record (MBR), the partition tables, and most of the files with random data. Once overwritten, the data are not recoverable.

Based on initial reporting and analysis of the malware, no evidence exists that Shamoon specifically targets industrial control systems (ICSs) components or U.S. government agencies.

According to Symantec,[a] Shamoon has three primary functional components:

1. Dropper—the main component and source of the original infection. It installs a number of other modules.
2. Wiper—this module is responsible for the destructive functionality of the malware.
3. Reporter—this module is responsible for reporting infection information back to the attacker.

After the initial infection, Shamoon spreads via network shares to infect additional machines on the network. Symantec first detected Shamoon on August 16, 2012, and estimates only few infections exist worldwide (less than 50).[b]

Organizations that observe any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT and US-CERT for tracking and correlation against other incidents.

IMPACT

Because of the highly destructive functionality of the Shamoon "Wiper" module, an organization infected with the malware could experience operational impacts including loss of intellectual property (IP) and disruption of critical systems. Actual impact to organizations vary, depending on the type and number of systems impacted.

a. http://www.symantec.com/connect/blogs/shamoon-attacks, Web site last accessed October 16, 2012.

b. http://www.symantec.com/security_response/writeup.jsp?docid=2012-081608-0202-99&om_rssid=sr-mixed30days, Web site last accessed October 16, 2012.

MITIGATION

ICS-CERT and US-CERT recommend the following mitigation strategies.

TACTICAL MITIGATIONS

--------- Begin Update B Part 1 of 1 --------

- Drill your recovery plans.
- Implement detection for internal network traffic matching previous Shamoon variant requests such as:
  http://<internal_C&C_IP>/ajax_modal/modal/data.asp?mydata=<_iteration>&uid=<IP>&state=<random number>
- Presence of the ElRawDisk driver on your system

--------- End Update B Part 1 of 1 ---------

- Encourage users to transfer critical files to network shares, to allow for central backed up.
- Execute daily backups of all critical systems.
- Periodically execute an “offline” backup of critical files to removable media.
- Establish emergency communications plans should network resources become unavailable.
- Isolate any critical networks (including operations networks) from business systems.
- Identify critical systems and evaluate the need for having on-hand spares to quickly restore service.
- Ensure antivirus is up to date. ICS-CERT is aware of antivirus reports that are not detecting some variants; however, updating signatures is still prudent.
- Disable credential caching for all desktop devices with particular importance on critical systems such as servers and restrict the number of cached credential for all portable devices to no more than three if possible. This can be accomplished through a Group Policy Object (GPO).
- Disable AutoRun and Autoplay for any removable media device.
- Prevent or limit the use of all removable media devices on systems to limit the spread or introduction of malicious software and possible exfiltration data, except where there is a

valid business case for use. This business case must be approved by the organization Chief IT Security Officer, with policy/guidance on how such media should be used.[c]

- Consider restricting account privileges. It is our recommendation that all daily operations should be executed using standard user accounts unless administrative privileges are required for that specific function. Configure all standard user accounts to prevent the execution and installation of any unknown or unauthorized software. Both standard and administrative accounts should have access only to services required for nominal daily duties, enforcing the concept of separation of duties. Lastly, disable Web and email capabilities on administrative accounts. Compromise of admin accounts is one vector that allows malicious activity to become truly persistent in a network environment.
- Ensure that password policy rules are enforced and Admin password values are changed periodically.
- Consider prohibiting hosts within the production environment or DMZ from sharing an Active Directory enterprise with hosts on other networks. Each environment should have separate forests within Active Directory, with no trust relationships allowed between the forests if at all possible. If necessary, the trust relationships should be one-way with the low integrity environment trusting the higher integrity environment.
- Consider deployment of a coaching page with click through acceptance; these are traditionally deployed in an environment to log the acceptance of network acceptable use policy or to notify users of monitoring. Coaching pages also provide some measure of protection from automated malicious activity. This occurs because automated malware is normally incapable of physically clicking an acceptance radial button. Automated malware is traditionally hardcoded to execute, then retrieve commands or additional executables from the Internet. If the malware is unable to initiate an active connection, the full train of infection is potentially halted. The danger still exists that the physical user will authorize access, but through the use of coaching pages, infections can be limited or at least the rate of infection reduced.
- Monitor logs—Maintain and actively monitor a centralized logging solution that keeps track of all anomalous and potentially malicious activity.
- Ensure that all network operating systems, web browsers, and other related network hardware and software remain updated with all current patches and fixes.

c.Using Caution with USB Drives, http://www.us-cert.gov/cas/tips/ST08-001.html, Web site last accessed October 16, 2012.

STRATEGIC MITIGATIONS

- Always keep your patch levels up to date, especially on computers that host public services accessible through the firewall, such as HTTP, FTP, mail, and DNS services.
- Build host systems, especially critical systems such as servers, with only essential applications and components required to perform the intended function. Any unused applications or functions should be removed or disabled, if possible, to limit the attack surface of the host.
- Implement network segmentation through V-LANs to limit the spread of malware.
- Consider the deployment of Software Restriction Policy set to only allow the execution of approved software (application whitelisting)
- Recommend the whitelisting of legitimate executable directories to prevent the execution of potentially malicious binaries.
- Consider the use of two-factor authentication methods for accessing privileged root level accounts or systems.
- Consider deploying a two-factor authentication through a hardened IPsec/VPN gateway with split-tunneling prohibited for secure remote access.
- Deny direct Internet access, except through the use of proxies for Enterprise servers and workstations. Perform regular content filtering at the proxies or external firewall points of presence. Also consider the deployment of an explicit versus transparent proxy policy.
- Implement a Secure Socket Layer (SSL) inspection capability to inspect both ingress and egress encrypted network traffic for potential malicious activity.
- Isolate network services, such as email and Web application servers by utilizing a secure multi-tenant virtualization technology. This will limit the damage sustained from a compromise or attack of a single network component.
- Implement best practice guidance and policy to restrict the use of non-Foundation assets for processing or accessing Foundation-controlled data or systems (e.g., working from home, or using a personal device while at the office). It is difficult to enforce corporate policies, detect intrusions, and conduct forensic analysis or remediate compromises on non-corporate owned devices.
- Implement best practice guidance and policy to limit the use of social networking services at work, such as personal email, instant messaging, Facebook, Twitter, except where there is a valid business case for use, and this business case has been approved by the organization Chief IT Security Officer. If a valid business case exists for use, implement a guidance/policy that reduces the risk of data loss and malware threats.

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[d]
- Place control system networks behind firewalls, and isolate or air gap them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.
- ICS-CERT and US-CERT remind organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.
- ICS-CERT recommends that organizations review the ICS-CERT Technical Information Paper ICS-TIP-12-146-01A Cyber Intrusion Mitigation Strategies[e] for high-level strategies that can improve overall visibility of a cyber intrusion and aid in recovery efforts should an incident occur.
- ICS-CERT also provides a recommended practices section for control systems on the US-CERT Web site. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[f]

CONTACT INFORMATION

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For industrial control systems security information and incident reporting: www.ics-cert.org

For any questions related to this report, please contact US-CERT at:

Email: soc@us-cert.gov
US-CERT Voice: 1-888-282-0870
ICS-CERT Watch Floor: 877-776-7585
Incident Reporting Form: https://forms.us-cert.gov/report/

d. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-343-01.pdf, Web site last accessed October 16, 2012.

e. ICS-CERT TIP—Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed October 16, 2012.

f. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed October 16, 2012.

DOCUMENT FAQ

What is a JSAR Advisory? A JSAR Advisory is a Joint Security Advisory intended to provide awareness or solicit feedback from critical infrastructure owners, integrators, peers, and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

May I edit this document to include additional information? This document may not be edited or modified in any way by recipients nor may any markings be removed. All comments or questions related to this document should be directed to either ICS-CERT or US-CERT at:

ICS-CERT: ics-cert@dhs.gov

US-CERT: soc@us-cert.gov