US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Technical Information Paper-TIP-11-103-01
Coreflood Trojan Botnet

Overview

Software vulnerabilities are not always a necessity for malicious software (malware) infection and propagation. The Coreflood Trojan is an example of this type of vulnerability-independent malware. It is designed to leverage the natural structure of a Windows network for account compromise and data theft.

Criminals typically utilize infected websites to stealthily infect users. Once the system is infected, the malware remains dormant on the system until someone with a privileged account (system administrator) logs in. Once the system administrator logs into the computer, the malware attempts to traverse the network using a legitimate Windows program, `psexec`. Later versions of the malware stopped using the `psexec` tool and implemented a custom tool designed to imitate `psexec` capabilities. Coreflood was originally discovered in 2001 and continues to evolve as an active threat within the malware market.

While it is possible for home users to become infected with the Coreflood Trojan, this threat is designed to infiltrate networks of larger organizations. Organizations may use the following indicators to determine a possible infection:

- Unusual usage of `ADMIN$`
- Intrusion detection sensor (IDS) alerts based on malware POST activity (reference the SecureWorks write-up linked below).
- Presence of `mng [12].log` files in `\<user>\Local Settings` folder. These log files identify successful and failed propagation attempts.

Suggested Mitigations

US-CERT recommends organizations evaluate the following tactical and strategic mitigations to determine which mitigations they can leverage in their specific environments to minimize and prevent Coreflood Trojan infections.

Tactical Mitigations

- When creating administrative accounts, restrict privileges and services to only those options required to perform their particular administrative duties. Keep in mind the concept of "Separation of Duties". This approach can help limit the damage that a single compromised administrative account can inflict on a system.
- Ensure that anti-virus products are properly deployed through out the network, including servers and workstations, with current virus definitions loaded for all products.
- Standardize user account privileges to restrict access to only required resources; restrict users from installing or running unknown or unauthorized applications.
- Ensure that all system-wide network operating systems, web browsers, and other related network hardware and software stay up to date with all current patches and fixes.
- Enforce a strong password policy for accessing network resources throughout the enterprise environment such as:
  - Minimum password length of eight characters for standard users.
  - Minimum password length of 15 characters for privileged accounts.
  - Use of alpha-numeric passwords.
  - Enable password history limits to prevent the reuse of previous passwords.
  - Prevent the use of personally-derived information as passwords, such as phone numbers and dates of birth.
  - Require password changes every 60-90 days.

Strategic Mitigations

- Consider using the two-factor authentication method for accessing privileged accounts.
- Establish a baseline for normal network performance and then review traffic patterns against the baseline to identify potential points of attack.
- Consider software restriction policies to allow only the execution of approved software.

References and Removal Tools

Additional information on this threat is available from the following resource:

- http://www.secureworks.com/research/threats/coreflood-report

The links listed below provide some suggested removal methods from various anti-virus vendors.

- http://www.symantec.com/security_response/writeup.jsp?docid=2003-090419-1001-99&tabid=3
- http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=100312
- http://www.sophos.com/support/knowledgebase/article/112129.html
- http://www.secureworks.com/research/threats/coreflood-removal/?threat=coreflood-removal

If users apply the SecureWorks method “Coreflood Removal for the Network Administrator”, modifications to the POST path in the Perl script may be required to work against different variants of the Trojan.

Contact US-CERT

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

E-mail: soc@us-cert.gov
Voice: 1-888-282-0870
Incident Reporting Form: https://forms.us-cert.gov/report/

Document FAQ

What is a TIP? A Technical Information Paper (TIP) is issued for a topic that is more informational in nature, describing an analysis technique, case study, or general cybersecurity issue. Depending on the topic, this product may be published to the public website.

If this document is labeled as UNCLASSIFIED, can I distribute it to other people? Yes, this document is intended for broad distribution to individuals and organizations interested in increasing their overall cybersecurity posture.

Can I edit this document to include additional information? This document is not to be edited, changed or modified in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov