US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

South Korean Malware Attack

Executive Summary

Reporting and technical details surrounding the malware used in the March 20, 2013, attack on South Korean assets have been varied and inconsistent. However, there are some commonalities reported across multiple organizations that provide some level of insight into the malware, dubbed DarkSeoul.

The common attributes of the attack campaign are the following:

- The malicious file wipes the master boot record (MBR) and other files.
- The malware was hard coded with a specific execution date and time and searches machines for credentials with administrative/root access to servers.
- The malware is written to specifically target South Korean victims.
- The attack is effective on multiple operating systems.
- The design is low sophistication – high damage.

When assessing the potential risk to U.S. Critical Infrastructure and Key Resources (CIKR), it is important to understand that DarkSeoul appears to have been coded for a specific target in this case and designed to evade typical South Korean antivirus processes. As this malware is currently packaged, it is a low risk to U.S. CIKR, however, the concepts underpinning this attack would likely succeed in many common enterprise environments. For this reason, U.S. CIKR owners and operators should continue the best standard security practices to avoid infection and propagation of a wiper or other type of malware that may impact their systems.

Defensive Measures

Based on the common attributes detailed above, US-CERT reminds users and administrators of the importance of best practices to strengthen the security posture of their organization's systems. CIKR owners and operators should work toward a resilient network model that assumes such an attack will occur against their enterprise. The goal is to minimize damage, and provide pathways for restoration of critical business functions in the shortest amount of time possible.

- Encourage users to transfer critical files to network shares, to allow for centralized backups. Leverage technical solutions to automate centralized storage where possible to reduce reliance on end-user voluntary compliance.

- Execute daily backups of all critical systems, including offline and offsite copies of backup media.
- Periodically execute a practice data restoration from backups, including key databases to ensure integrity of existing backups and processes.
- Establish emergency communications plans should network resources become unavailable.
- Isolate any critical networks (including operations networks) from business systems, and where possible segment the business networks.
- Identify critical systems and evaluate the need to have on-hand spares to quickly restore service.
- Recognize that without proper internal monitoring, an organization's "Enterprise Trust Anchors" (Active Directory, PKI, two-factor authentication, etc.) and centralized management services (remote helpdesk access, patch management and asset inventory suites, etc.) could be compromised and used to subvert all other security controls.
- Maintain up-to-date antivirus signatures and engines.
- Restrict users' ability (permissions) to install and run unwanted software applications through Microsoft Software Restriction Policy (application directory whitelisting) or AppLocker, application whitelisting products, or host-based intrusion prevention software.
- Enforce a strong password policy and implement regular password changes.
- Keep operating system patches up to date.
- Disable unnecessary services on workstations and servers.
- Scan for and remove suspicious email attachments; ensure the scanned attachment is its 'true file type' (i.e., the extension matches the file header).
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs).
- Scan all software downloaded from the Internet prior to executing by properly authorized personnel.
- Disable credential caching for all desktop devices with particular importance on critical systems such as servers and restrict the number of cached credentials for all portable devices to no more than three, if possible. This can be accomplished through a Group Policy Object (GPO).

- Consider restricting account privileges. US-CERT recommends all daily operations should be executed using standard user accounts unless administrative privileges are required for that specific function. Both standard and administrative accounts should have access only to services required for nominal daily duties, enforcing the concept of separation of duties and least privilege/least access. Web and email capabilities should also be disabled on administrative accounts. Compromise of administrative accounts is one vector that allows malicious activity to become truly persistent in a network environment.