Appendix B: Technical Analysis of Custom Attack Tools

SecHack Sample

- KB77846376.exe (MD5: 47f9cc543905a69a423f9110ae7deffb)
    - Compiled: 2014-10-23T07:33:25Z
    - Includes 64-bit version of itself as a resource labeled "IDR_MOD1" (MD5: ee477fdee8b6ad4fe778a6fa4058f9aa)

SecHack (KB77846376.exe) is a credential theft utility that can extract passwords on 32- and 64-bit Windows operating systems from the memory of lsass.exe, similar to the Mimikatz sekurlsa::logonpasswords module::command. The malware can also survey the compromised system for information about the operating system version and its own process attributes and retrieve information about the installed certificates. The malware must be executed with elevated privileges to collect the information. An external tool or installer is required if the attacker desires persistence.

- The tool queries the following authentication packages:
    - msv1_0
    - kerberos
    - wdigest
    - tspkg
- SecHack accepts two optional parameters to query for additional data: "cert," "info," or both.
    - cert collects the following certificate information: store, subdir, name, container, provider, keyspec, key size, key exportable, pfx.
    - info collects the following system information: operating system version and full version, Product Name, Processor Architecture, UAC Admin flags, Current Process Attributes.
- If SecHack is executed within the context of a 64-bit process, it writes a 64-bit version of itself under the same full path name with the inclusion of the file extension ".x64."

Output is in JSON format and starts with "SecHack 1.0 by OSA" (Figure 4).

Figure 4: SecHack default output, snippet

Figure 5: SecHack info output, snippet

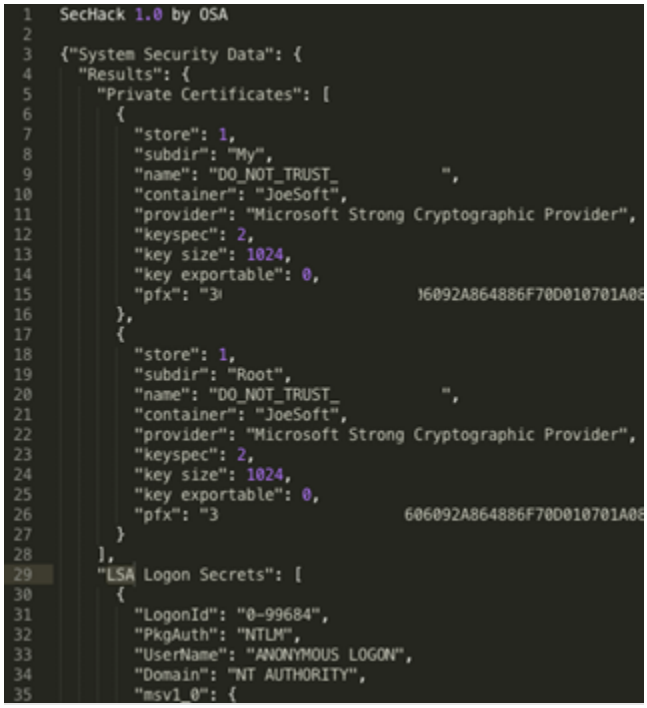

Figure 6: SecHack cert output, snippet

NetExec Sample

- netexec.exe (MD5: aca94bb7bdfb735f267f083e28f4db37)
    - Compiled 2015-09-01 07:37:04Z
    - Self-reported as Version 0.9

NetExec is a utility to execute a command or program on a remote system. The malware does not contain a persistence mechanism.

- NetExec can:
    - Execute remote files
    - Upload files from local machine to remote machine and execute
    - Open a remote command shell
    - Open a remote PowerShell instance
    - Copy itself to a remote machine
- When instructed to execute with --cmd or –ps, this sample copies an embedded runsvc.exe to the target system. This sample then executes the newly copied file. The embedded executable is an interactive application and runs either "cmd.exe" or "powershell.exe."
    - %WINDIR%\<System32/SysWOW64>\wbem\xml\runsvc.exe (MD5: 1904cad4927541e47d453becbd934bf0)
- Runsvc.exe leverages randomly named pipes to communicate with netsvc.exe.

Figure 7: NetExec version

Figure 8: NetExec use information

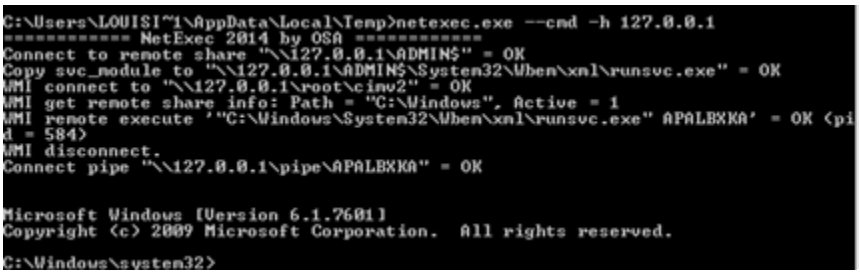

Figure 9: NetExec sample execution, cmd

Compattelprerunner.exe Sample

Cryptcat-Based Backdoor Component

- compattelprerunner.exe (MD5: 35F443608FC4EEB78F9347A9DFC5AEA1)
    - Compiled 2017-04-25 12:06:07

compattelprerunner.exe is a C2 domain name generator (DNG) that performs a DNS query for a generated hostname and launches an external program using the resolved IP address as an argument.

- When the malware launches, it performs a DNS query for the domain names "upd-%d.mooo.com" and "%d-srv.net." The format string %d is replaced with a value based on the current date. The DNS server the malware uses is "8.8.8.8."
- The algorithm for calculating the %d number is calculated by taking the date, month, and [year – 116]. Note that the year is captured using the "_localtime64" function. This function returns the year as a number incremented from 1900. Therefore, subtracting 116 means the current year is based on the year 2016. This is a possible indication when this DGA code was first authored.
    - 1/30/2018, therefore, becomes 3012. This is the [day][month][number of years since 2016]. This number is multiplied times itself, resulting in the value 9072144. So, the domain used for 1/30/2018 are "udp-9072144.mooo.com" and "9072144-srv.net."
- The malware creates two processes using the format string "cryptsvc.exe -e cmd %S 443." %S is replaced with the IP address returned from the two DNS queries for the generated domain names.

napupdatedb.exe Sample

PLINK-Based Backdoor Component

- napupdatedb.exe (MD5: BA51F25DB03A66C658D1FD4396F32843)
    - Compiled 2017-04-25 12:06:07

napupdatedb.exe is a modified PLINK (PUTTY) executable. This SSH-based backdoor initiates a reverse tunnel with embedded credentials to local port 3389, making RDP available on the attacker-controlled server over TCP port 8531.

- This sample contains a list of C2 servers and credentials to tunnel traffic. The embedded configuration is a ";" separated list of command-line arguments passing directly to PLINK.

    - The malware replaces the "*" character of each C2 domain with the six-digit local time on the infected system.

OpenSSH-Based Backdoor

spl32.exe is a modified and custom-compiled version of the sshd.exe from OpenSSH. When launched from a command line, spl32.exe listens on TCP port 50501. It was designed to be a self-contained executable with OpenSSL library built-in and no additional system dependencies.

- spl32.exe sample deviates from the original sshd.exe by having a fixed configuration and three hard-coded cryptokey pairs.
    - This backdoor included the WinSAT.exe component, an unmodified but custom-compiled version of sftp-server.exe from OpenSSH.
    - WinSAT is launched by spl32.exe when an inbound sftp connection is made and accepted by spl32.exe.

Bitvise-Based Backdoor

Bitvise is frequently used for file transfer and can achieve high transmission speeds through the SFTP subcomponent. It has an obfuscation option that, when supported and enabled in both the client and server, makes it more difficult for an observer to detect that the protocol being used is SSH.