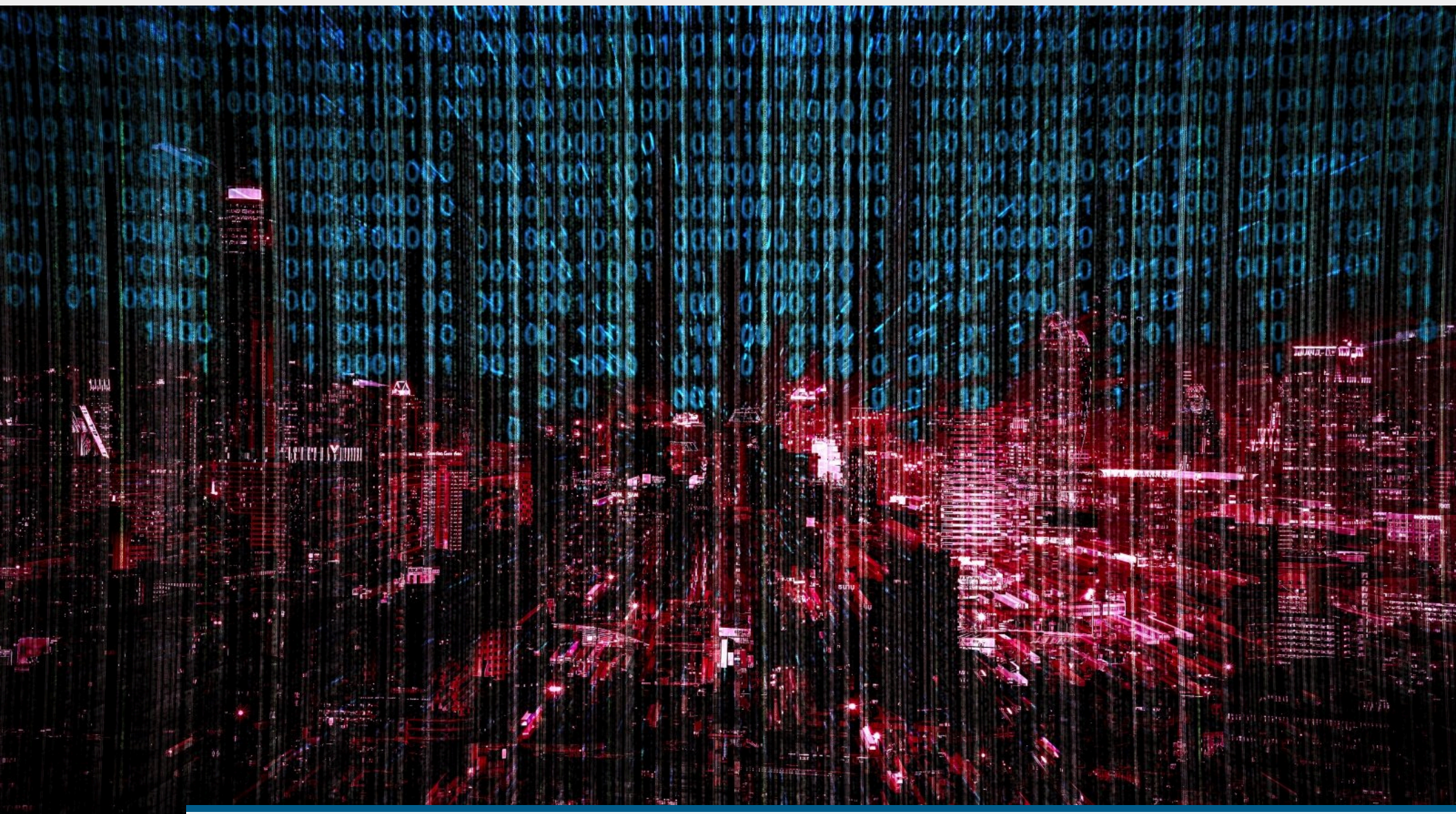

Threat Hunter Team
Symantec

POSTED: 13 SEP, 2022 | 12 MIN READ |
THREAT INTELLIGENCE

TRANSLATION: 日本語

SUBSCRIBE FOLLOW

New Wave of Espionage Activity Targets Asian Governments

Governments and state-owned organizations are the latest targets of a well-established threat actor.

A distinct group of espionage attackers who were formerly associated with the ShadowPad remote access Trojan (RAT) has adopted a new, diverse toolset to mount an ongo
in a num
early 20

Targ

The curr
public e

SHARE

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our Cookie Policy.

Accept Cookies

Cookies Settings

- Head of government/Prime Minister's Office
- Government institutions linked to finance
- Government-owned aerospace and defense companies
- State-owned telecoms companies
- State-owned IT organizations
- State-owned media companies

Tools

A notable feature of these attacks is that the attackers leverage a wide range of legitimate software packages in order to load their malware payloads using a technique known as DLL side-loading. Usually, the attackers used multiple software packages in a single attack. In many cases, old and outdated versions of software are used, including security software, graphics software, and web browsers. In some cases, legitimate system files from the legacy operating system Windows XP are used. The reason for using outdated versions is that most current versions of the software used would have mitigation against side-loading built-in.

DLL side-loading is a well-known technique that involves attackers placing a malicious DLL in a directory where a legitimate DLL is expected to be found. The attacker then runs the legitimate application themselves (having installed it themselves in most cases). The legitimate application then loads and executes the payload.

Once a malicious DLL is loaded by the attackers, malicious code is executed, which in turn loads a .dat file. This file contains arbitrary shellcode that is used to execute a variety of payloads and associated commands in memory. In some cases, the arbitrary shellcode is encrypted.

The attackers also leverage these legitimate software packages to deploy additional tools, which are used to further aid in lateral movement. These tools include credential dumping tools, a number of network scanning tools (NBTScan, TCPing, FastReverseProxy, and FScan), and the Ladon penetration testing framework.

Attacks usually unfold in the following manner:

- Once backdoor access is gained, the attackers use Mimikatz and ProcDump to steal credentials. I
- They then use netv
such as those runn
- They leverage PsE
used to load additi
loading on other c
- The attackers also
mount snapshots of Active Directory servers in order to gain access to Active

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our **Cookie Policy.**

Directory databases and log files. The Dnscmd command line tool is also used to enumerate network zone information.

Case Study: An unfolding attack

In April 2022, the attackers targeted a government-owned organization in the education sector in Asia and managed to stay on its network until July. During the period of the compromise, the attackers accessed computers hosting databases and emails and eventually made their way to the domain controller.

The first sign of malicious activity occurred on April 23, when a malicious command was executed via imjpuex.exe (SHA256: fb5bc4baece5c3ab3dabf84f8597bed3c3f2997336c85c84fdf4beba2dcb700f). The file imjputyc.exe is a legitimate Windows XP file that was used by the attackers to side-load a malicious DLL file (imjputyc.dll), which in turn was used to load a .dat file (payload - imjputyc.dat). Following this activity, imjputyc.exe was used to launch a network service via svchost.exe, likely created by the malicious payload.

- CSIDL_SYSTEMX86\svchost.exe NetworkService 7932

Additionally, around the same time, the attackers leveraged Imjpuex.exe to install and execute an eleven-year-old version of Bitdefender Crash Handler (file name: javac.exe, SHA256: 386eb7aa33c76ce671d6685f79512597f1fab28ea46c8ec7d89e58340081e2bd). While Crash Handler was used for side-loading in this attack, it is just one of many old versions of applications that have been used by this group in recent months.

The same Crash Handler executable was copied to CSIDL_SYSTEM_DRIVE\xampp\tmp\vmware.exe and executed.

The attackers then installed and executed ProcDump in order to dump credentials from the Local Security Authority Server Service (LSASS):

- p.exe -accepteula -ma lsass.exe lsass2.dmp

The attackers then launched several command prompts while reloading Crash Handler. This was likely done in order to install additional tools.

Shortly afterwards, a fi
912018ab3c6b16b39e
appeared on the mach
version of Mimikatz tha

- calc.exe ""privileg

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our **Cookie Policy.**

On April 26, further malicious activity occurred when the attackers ran the Crash Handler executable and installed a file called cal.exe (SHA256: 12534f7014b3338d8f9f86ff1bbeacf8c80ad03f1d0d19077ff0e406c58b5133) on the compromised machine.

This file was LadonGo v3.8, a publicly available penetration testing framework that is written in Go. The attackers appear to have used LadonGo to scan the internal network for machines with RDP services running and attempted to exploit or log in to those machines using the credentials they stole several days earlier. There was also some evidence of brute-force login attempts against machines of interest.

On May 6, the attackers resumed their attack and ran the Crash Handler executable (this time named svchost.exe) and installed a new variant of Mimikatz named test.exe (SHA256: 912018ab3c6b16b39ee84f17745ff0c80a33cee241013ec35d0281e40c0658d9). This was likely done in order to obtain more credentials. The attackers then ran LadonGo and attempted to exploit a Netlogon vulnerability (CVE-2020-1472) against two other computers in the organization in order to elevate privileges.

On May 16, the attackers increased their level of activity and began moving laterally across the organization's network from the initially compromised computer (Computer #1).

On a second computer (Computer #2), the attackers launched a command prompt and executed a variant of Mimikatz (file name: test.exe, SHA256: 912018ab3c6b16b39ee84f17745ff0c80a33cee241013ec35d0281e40c0658d9). The attackers then deployed a number of Knowledge Base files (e.g. kb0394623.exe) on the computer. These files are legitimate copies of the Windows command prompt (with 16 bytes of the rich header modified).

On a third computer (Computer #3) the attackers used PsExec to execute the same older version of Crash Handler used on Computer #1, this time named javac.exe. A copy of this executable was then made to csidl_program_files\windows mail\winmailservice.exe and was executed.

The attackers then ran dnscmd.exe (SHA256: 67877821bf1574060f4
which was used to enu
computer:

- Dnscmd . /EnumZ

Dnscmd is a Microsoft
to script batch files to
routine setup of new DNS servers. The enumzones command is used to list the zones

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our **Cookie Policy.**

that exist on the specified DNS server. If no filters are specified, a complete list of zones is returned.

Crash Handler was then used to install imjpuex.exe in the csidl_common_appdata\veritas directory which in turn was used to side-load a DLL file of the same name and load a .dat file to execute an unknown custom payload.

Shortly after this, the attackers attempted to list the records of multiple specific zones by specifying the domain on the command line:

- Dnscmd . /ZonePrint [REDACTED_DOMAIN]

On a fourth computer (Computer #4), the attackers used PsExec to execute Crash Handler (this time named test.exe). They then installed and executed two KB files in the %TEMP% directory.

- SHA256: 5c4456f061ff764509a2b249f579a5a14d475c6714f714c5a45fdd67921b9fda
- SHA256: ded734f79058c36a6050d801e1fb52cd5ca203f3fd6af6ddea52244132bd1b51

Again, both of these files were modified versions of the Windows command prompt.

On May 17, the attackers deployed several more modified Windows command prompt applications on Computer #4. They also deployed the side-loading technique on Computer #5 to execute the legitimate svchost.exe application, possibly to facilitate some process injection.

On May 19, the attackers returned to Computer #5 and used svchost to launch NetworkService. The attackers then used a variant of Mimikatz named calc.exe, which was previously used earlier in the attack (SHA256: 912018ab3c6b16b39ee84f17745ff0c80a33cee241013ec35d0281e40c0658d9). Mimikatz was used to dump credentials from the compromised host.

On May 24, the attackers turned their attention to Computer #3, using PsExec to execute the whoami command and determine the currently logged-in user. They then ran an unknown batch file name t.bat via PsExec.

It is likely the following
new user account:

- net user [REDACT
- CSIDL_SYSTEM\r
- net localgroup [RE
- CSIDL_SYSTEM\r

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our **Cookie Policy.**

- CSIDL_SYSTEM\net1 user [REDACTED] Asd123.aaaa /add

The script uses net.exe to check if a specific user account already exists. It then attempts to create a user account with the password Asd123.aaaa and add it to the local group on the machine. Several minutes later, the task manager was launched followed by a command prompt. The attackers then ran the following command to mount a snapshot of the active directory server.

- ntdsutil snapshot "mount c2b3e2c6-1ffb-4625-ba8e-3503c27a9fcb" quit quit

These snapshots contain sensitive information such as the active directory database (i.e. user credentials) and log files. The string c2b3e2c6-1ffb-4625-ba8e-3503c27a9fcb is the index number of the snapshot.

The attackers then moved to Computer #5, where they used ProcDump (file name: p.exe, SHA256: 2f1520301536958bcf5c65516ca85a343133b443db9835a58049cd1694460424) to dump credentials from LSASS:

- p.exe -accepteula -ma lsass.exe lsass2.dmp

On May 26, the attackers returned to Computer #1 and executed a file called go64.exe. This file was a copy of Fscan. The attackers ran the following command to mass scan for any machines within the compromised network (specifically a class C scan against machines in the IP range 10.72.0.0 → 10.72.0.255) with RDP services:

- go64.exe -h 10.72.0.101/24 -pa 3389

There is also evidence that the attackers leveraged Fscan in order to perform exploit attempts against other machines on the network, including leveraging one of the ProxyLogon vulnerabilities (CVE-2021-26855) against an Exchange Server.

Suspicious SMB activity also occurred around this time, suggesting the attackers may have also leveraged other exploits (likely EternalBlue) against any open SMB services.

On June 6, the attackers ran PsExec on Computer #3 to launch the previously used old version of Crash Handler (file name: winnet.exe) from the %USERPROFILE%\pu

They ran the Dnscmd u
winnet.exe again and a
additional malicious pa

- Dnscmd . /EnumZ
- "CSIDL_COMMON

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our **Cookie Policy.**

Several hours later, ProcExplorer (64-bit) was launched:

- "CSIDL_PROFILE\desktop\processexplorer\procexp64.exe"

The last known malicious activity occurred on July 8 on Computer #3. The system hive file was dumped from the registry in order to dump user credentials.

- reg save HKLM\SYSTEM system.hiv

Payloads

While this group of attackers was previously using ShadowPad, it has since moved on and has been deploying a range of payloads.

One of the payloads used was a previously unseen, feature-rich information stealer (Infostealer.Logdatter), which appeared to be custom built. Its capabilities included:

- Keylogging
- Taking screenshots
- Connecting to and querying SQL databases
- Code injection: Reading a file and injecting the contained code into a process
- Downloading files
- Stealing clipboard data

Other payloads used by the attackers included:

- PlugX/Korplug Trojan
- Trochilus RAT
- QuasarRAT
- Ladon penetration testing framework
- Nirsoft Remote Desktop PassView: A publicly available tool that reveals the password stored by the Microsoft Remote Desktop Connection utility inside .rdp files
- A Simple Network Management Protocol (SNMP) scanning tool
- Fscan: A publicly available intranet scanning tool
- Nbtscan: A command-line tool that scans for open NETBIOS name servers
- FileZilla: A legitimate FTP client
- FastReverseProxy
- WebPass: A publi
- TCPing: A publicly
- Various process d
- Various keylogger
- A number of Powe

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our **Cookie Policy.**

Links to earlier activity

ShadowPad is a modular RAT that was designed as a successor to the Korplug/PlugX Trojan and was, for a period of time, sold on underground forums. However, despite its origins as a publicly available tool, it has since been closely linked to espionage actors. The tool was only sold publicly for a very short period of time and it is believed that it was only sold to a handful of buyers.

There is limited evidence to suggest links to past attacks involving the Korplug/PlugX malware and to attacks by a number of known groups, including Blackfly/Grayfly (APT41) and Mustang Panda. For example, the attackers leveraged a legitimate file called HPCustParticUI.exe, which was developed by HP for digital imaging applications. This previously occurred in attacks involving Korplug/Plug X. Furthermore, the attackers used a file called hpcustpartui.dll as a likely loader. The same loader was used in a long-running campaign involving Korplug/Plug X targeting the Roman Catholic Church.

The current campaign uses a legitimate Bitdefender file to side-load shellcode. This same file and technique were observed in previous attacks linked to APT41. We have also observed the same keylogging tool deployed in previous attacks against critical infrastructure in South East Asia.

The use of legitimate applications to facilitate DLL side-loading appears to be a growing trend among espionage actors operating in the region. Although a well-known technique, it must be yielding some success for attackers given its current popularity. Organizations are encouraged to thoroughly audit software running on their networks and monitor for the presence of outliers, such as old, outdated software or packages that are not officially used by the organization.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

Legitimate applicatio

386eb7aa33c76ce671

Bitdefender Crash Har

Loaders

1a95c0b8046aafa8f94

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our **Cookie Policy.**

138c82c81ed7b84378a821074c88157c489d29d5ef66080baea88f5de0e865e6 – log.dll

704e6eb9bded6d22feab88fa81e6b0b901bee7a451a290c20527c48c235ebf52 – breakpad.dll

7a25b21df9fa93a694f15d18cd81c9f9be6fc078912924c91c645f75a5966881 – breakpad.dll

1d6aabf2114f9e6367b515d4ebfc6e104511ff4b05bd51a56fa52070c1d40e25 – breakpad.dll

5bedd1b05879b900b60a07abc57fab3075266ee7fa72385ced582699a51f1ec7 – breakpad.dll

49c23a187810edd3c16689ee1766445ec49a7221507dbe51e7b5af8ec46a91ee – breakpad.dll

e51fc50defd89da446ddc0391e53ace60b016e497c5cb524fd81efdeadda056d – breakpad.dll

Payloads

2237e15b094983a79f60bc1f7e962b7fb63aae75cbf5043ee636be4c8fdb9bee – Korplug

b7f6cf8a6a697b254635eb0b567e2a897c7f0cefb0c0d4576326dc3f0eb09922 – Korplug

1c7e2d6ae46ff6c294885cb7936c905f328b303d6f790b66d7c4489f284c480a – QuasarRAT

c3ae09887659cde70d636157c5a0efd36359efdfb2fe6a8e2cdd4e5b37528f51 – TrochilusRAT

Additional tools

fa7eee6e322bfad1bb0487aa1275077d334f5681f0b4ede0ee784c0ec1567e01 – NBTScan

d274190a347df510edf
NBTScan

20c767d32304ed2812
NBTScan

cf5537af7dd1d0dbb77
NBTScan

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our **Cookie Policy.**

df9a2471c23790a381e286bb96ea3401b94686b7ca067297a7920a76a7202112 – Loader

05fb86d34d4fa761926888e5347d96e984bbb1f3b693fe6c3ab77edb346f005b – FScan

aba3e885768a6436b3c8bc208b328620f001c63db7a3efe6142e653cdf5dfbf7 – FScan

0f81c3850bc82a7d1927cf16bfad86c09414f8be319ef84b44a726103b7d029d – Powerview

9f04c46e0cdaa5bce32d98065e1e510a5f174e51b399d6408f2446444cccd5ff – TCPing

12534f7014b3338d8f9f86ff1bbeacf8c80ad03f1d0d19077ff0e406c58b5133 – Ladon

23d0eff3c37390d38e6386a964c88ac2dafbace92090a762ae9e23bd49510f09 – WebPass

3e53deb5d2572c0f9fae10b870c8d4f5fdc7bd0fe1cc3b15ca91b31924373136 – WebPass

2f1520301536958bcf5c65516ca85a343133b443db9835a58049cd1694460424 – ProcDump

912018ab3c6b16b39ee84f17745ff0c80a33cee241013ec35d0281e40c0658d9 – Mimikatz

38d4456b38a2896f23cad615e3c9167e65434778074a9b24af3cbc14d1e323bf – cmd.exe (tampered copy of legitimate cmd.exe)

77358157efbf4572c2d7f17a1a264990843307f802d20bad4fb2442245d65f0b – ProcessExplorer

Network

88.218.193.76 (used to host malware)

8.214.122.199

103.56.114.69

27.124.17.222

27.124.3.96

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our **Cookie Policy.**

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

Want to comment on this post?

We encourage you to share your thoughts on your favorite social platform.

Related Blog Posts

POSTED: 22 OCT, 2024 | 5 MIN READ

Exposing the Danger Within: Hardcoded Cloud Credentials in Popular Mobile Apps

POSTED: 17 OCT, 2024 | 3 MIN READ

Ransomware: Threat Level Remains High in Third Quarter

POSTED: 2 OCT, 2024 | 5 MIN READ

Stonefly: Extortion Attacks Continue Against U.S. Targets

POSTED: 12 SEP, 2024 | 3 MIN READ

Ransomware: Attacks Once More Nearing Peak Levels

SUBSCRIBE FOLLOW

Privacy Policy Cookie Policy Data Processing and Data Transfers Supplier Responsibility Terms of Use Sitemap

Copyright © 2005-2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our **Cookie Policy.**