Blackgear Cyberespionage Campaign Resurfaces

By By: Joey Chen Jul 17, 2018 Read time: 6 min (1675 words)

Published: 2018-07-17 · Archived: 2026-04-05 15:26:43 UTC

Blackgear (also known as Topgear and Comnie) is a cyberespionage campaign dating back to 2008open on a new tab, at least based on the Protux backdoor used by its operators. It targets organizations in Japan, South Korea, and Taiwan, leveling its attacks on public sector agencies and telecommunications and other high-technology industries. In 2016, for instance, we found their campaigns attacking Japanese organizations with various malware tools, notably the Elirks backdoor. Blackgear's operators are well-organized, developing their own tools, which we observed to have been recently fine-tuned, based on their latest attacks.

A notable characteristic of Blackgear is the degree to which its attacks are taken to evade detection, abusing blogging, microblogging, and social media services to hide its command-and-control (C&C) configuration. Compared to when C&C information is embedded within the malware, where it's preset and can thus be easily blocked, this tactic lets Blackgear's operators to quickly change C&C servers as needed. It can, in turn, prolong the campaign's foothold in the system and enable attackers to carry out further lateral movement.

Analyzing the Marade downloader (detected by Trend Micro as TSPY_MARADE.ZTBC) and the version of Protux (BKDR_PROTUX.ZTBC) employed by Blackgear's latest campaigns, we found their encrypted configurations on blog and social media posts (see Figure 1). This can be an indication that these malware tools were developed by the same group.

intel*Figure 1. Marade's encrypted configuration on a Facebook post*

intel*Figure 2. Infection chain of Blackgear's attack*

Attack chain

To paint a bigger picture of Blackgear's attacks, we correlated the tools and tactics they used against their targets. Here's a summary of Blackgear's latest campaign:

1. Use a decoy document or fake installer file, sent via spam email to lure a potential victim into clicking it.
2. The decoy document will extract the Marade downloader. It drops itself in the machine's Temp folder and increases its file size to over 50MB in order to bypass traditional sandbox solutions.
3. Marade will check if the infected host can connect to the internet and if it is installed with anti-virus (AV) software.
4. If the affected system can connect online and doesn't have AV software, Marade will connect to a Blackgear-controlled public blog or social media post to retrieve an encrypted C&C configuration. Otherwise, Marade will use the C&C information embedded in its code.
5. The encrypted strings will pose as a magnet link to keep its malicious traffic from being detected by AV software. Marade will then decrypt the encrypted strings and retrieve the C&C server information.

6. The C&C server will send Protux to the victim's host and execute it. Protux, a known backdoor, is executed by abusing the *rundll32* dynamic-link library (DLL). It tests the host's network, retrieves the C&C server from another blog, and uses the RSA algorithm to generate the session key and send information to the C&C server.

Blackgear's malware tools are delivered to targets using RAR self-extracting executable (SFX) files or office Visual Basic Script (VBScript) to create a decoy document. Below is a screenshot of the SFX files and document used by the latest campaigns:

 *Figure 3. Contents of malicious SFX file used by Blackgear, posing as a Flash Player installer*

 *Figure 4. Malicious document used by Blackgear (top) and how VBScript is used to execute Marade (bottom)*

 *Figure 5. Encrypted configurations of Protux (top) and Marade (bottom) in the same blog post*

Correlating Marade and Protux

The encrypted configurations of Marade and Protux can both be found on a single blog post. As shown in Figure 5, the strings highlighted in red function as a search tag to identify the location of the configuration information; those highlighted in orange pertain to the encrypted configuration that Protux will retrieve.

In Blackgear's previous campaigns, Protux's configuration format had to be changed to another version. For instance, Protux's older iteration will look for the "++a++" tag, as shown in Figure 5. The format used by Protux's latest version is now similar to Marade's, as shown in Figure 6.

 *Figure 6. Protux's encrypted configuration on a public blog (note the six magnet URLs; the third is Protux's latest configuration format)*

Reverse analysis of Protux's latest version also allowed us to determine how to decrypt the C&C information, which is done in the Python code shown below. This can also be used by researchers, system administrators, and information security professionals when decrypting Protux's latest version.

```
#!/usr/bin/env python2

#-*-coding:utf-8 -*-

import os, sys, datetime, operator, base64

def decrypt():

if len(sys.argv) != 2:

print "Usegae : ./decrypt_protux_magnet.py <Full magnet strings>"

sys.exit(0)
```

```
str = sys.argv[1]

head = str.find("magnet:?xt=urn:bhih:")

tail = str.find("&xl=")

if -1 ==tail:

tail = str.find("&amp;xl=")

if -1 == head or -1 == tail:

print("can't find delimiter")

sys.exit()

b64_data = str[len("magnet:?xt=urn:bhih:"): tail]

b64_decode = base64.b64decode(b64_data)

key = ord(b64_decode[2])

data = b64_decode[4:]

output_file = open("C2_info", "wb")

for single_byte in data:

output_file.write(chr(ord(single_byte) ^ key))

output_file.close()

if __name__ == '__main__':

decrypt ()
```

A new remote controller tool

We were also able to source a sample of Protux's remote controller tool. This provides a user interface (UI) that allows attackers to send instructions to and monitor any compromised endpoint host. This tool can also remotely control Marade in the affected system.

intel

intel*Figure 7. The controller retrieving the Marade-related information (top) and collecting Protux-related information (bottom)*

Based on the controller's behavior, we can posit that both Marade and Protux were authored by the same threat actors. Each serves a specific role once in the system. Marade acts as the first stage of attack, sending the compromised system's information to the C&C server and then awaiting commands from the controller. This

allows threat actors to monitor and check whether the affected system is of interest to them. If so, the attack moves to the second stage by deploying Protux. The tool can also control the communication between the backdoor and attacker in real time. The following is a list of Protux's notable components and their functions:

- *FileManage* - Lists all of the system's drives and folders.
- *ProcManage* - Lists all of the processes, modules, threads, and ports in the compromised host.
- *ServiceManage* - Lists all of the services in the compromised host.
- *RegManage* - Lists all of the registries in the compromised host.
- *ScreenManage* - Takes a screenshot.
- *ShellManage* - Creates a shell.

Protux: An old dog learning new tricks

Protux is an old backdoor, with its first version developed in 2005. It uses DLL injection to execute its routines. Based on this behavior, we can map out a pattern, from the downloader to the decoy documents used. The trigger format is: *%system32/rundll32.exe <PROTUX file name> <export name>*.

We saw two notable changes throughout Protux's history: its export name and how it functions:

Export name	**Year**	**How C&C information is retreieved**
TStartUp	2005 – 2012	Directly connect to the C&C server and use DNS server to retrieve the C&C IP address.
CRestart	2009 – 2014	Use web DNS query to retrieve the C&C IP address, e.g., ip138[.]com.
CReset	2013 – 2018	Find the encrypted configuration through keywords on blog services.

Our research into and correlation of Protux led us to several samples that have version numbers embedded in them. The highlighted portions in Figure 8 show the backdoor's version number and timestamp with the "with encrypt" strings. We also found that these versions encrypt the communication to its C&C servers.

Protux's latest version, 3.7, uses the open-source compiler OpenCSP to generate a session key with the RSA algorithm.

intel intel intel*Figure 8. Different versions of Protux used by Blackgear*

intel*Figure 9. Protux with the OpenCSP encryption function*

Building a proactive incident response strategy

Blackgear has been targeting various industries since its emergence a decade ago. Its apparent staying power stems from the furtive ways with which its attacks can evade traditional security solutions. For instance, Blackgear employs two stages of infection for each of its attacks. The potential victim may not be able to notice

the intrusions as the first stage involves only profiling and reconnaissance. And once infection with a backdoor occurs, typical red flags may not be raised as it abuses microblogging and social media services to retrieve information needed for C&C communication.

Indeed, Blackgear's attacks exemplify the need for organizations to develop and implement security strategies that can proactively respond to threats. A robust threat hunting strategyproducts, for instance, helps validate indicators of attack to ascertain if the intrusions, threats, or suspicious system activities are one-off attacks or part of a larger campaign. This further visibility equips organizations with actionable threat intelligencenews- cybercrime-and-digital-threats, context, and insights that can be used to delve deeper into an attack — which security gaps are exploited, if the attack has multiple payloads, or if the malware has already spread within the network.

Organizations can also consider managed detection and response, which provides in-depth threat analysis and correlation — from networks to servers and endpoints — to obtain a complete picture of and further understand a targeted attack. Managed detection and response also helps make better sense of system- and network-level activities that an organization may not have the time or resources to do.

A list of indicators of compromise (IoCs) related to Blackgear is in this appendixopen on a new tab.

Trend Micro solutions

The Trend Micro™ Deep Discovery™products solution provides detection, in-depth analysis, and proactive response to today's stealthy malware and targeted attacks in real time. It provides a comprehensive defense tailored to protect organizations against targeted attacks and advanced threats through specialized engines, custom sandboxingopen on a new tab, and seamless correlation across the entire attack life cycle, allowing it to detect threats delivered by Blackgear even without any engine or pattern update.

Blackgear's campaigns also use email as an entry point, which is why it's important to secure the email gateway. The Trend Micro™ Hosted Email Securityproducts no-maintenance cloud solution delivers continuously updated protection to stop spam, malware, spear phishing, and advanced targeted attacks before they reach the network. The Trend Micro™ Deep Discovery™ Email Inspectorproducts and InterScan™ Web Securityproducts solutions prevent malware from ever reaching end users. At the endpoint level, the Trend Micro™ Smart Protection Suitesproducts deliver several capabilities that minimize the impact of attacks.
