Trochilus RAT Evades Antivirus Detection, Used for Cyber-Espionage in South-East Asia

news.softpedia.com/news/trochilus-rat-evades-antivirus-detection-used-for-cyber-espionage-in-south-east-asia-498776.shtml

Catalin Cimpanu

January 12, 2016

A new type of RAT (Remote Access Trojan) has been discovered in use against governments and civil society organizations in South-East Asia, the Arbor Security Engineering & Response Team (ASERT) at Arbor Networks reports.

This particular RAT has been linked to a previous campaign against the Myanmar government that was unmasked by both Arbor Networks' and Cisco's security teams at the end of August 2015.

During that campaign, the threat actor identified as Group 27 used watering hole attacks on official Myanmar government websites to infect unsuspecting users with the PlugX malware (an RAT) when accessing information on the upcoming Myanmar elections.

Myanmar cyber-espionage campaign continued, even after it was made public

Arbor's ASERT team is now reporting that, after looking deeper at that particular campaign, and by exposing a new trail in the group's activities, they managed to identify a new RAT that was undetectable at that time by most antivirus vendors.

Named Trochilus, this new RAT was part of Group 27's malware portfolio that included six other malware strains, all served together or in different combinations, based on the data that needed to be stolen from each victim.

This collection of malware, dubbed the Seven Pointed Dagger by ASERT experts, included two different PlugX versions, two different Trochilus RAT versions, one version of the 3012 variant of the 9002 RAT, one EvilGrab RAT version, and one unknown piece of malware, which the team has not entirely decloaked just yet.

According to the security experts, this collection of malware was discovered after their first initial report was published, meaning that Group 27 ignored the fact they were unmasked and continued to infect their targets regardless, through the same entry point, the Myanmar Union Election Commission (UEC) website. Trochilus RAT activity was discovered during both months of October and November 2015.

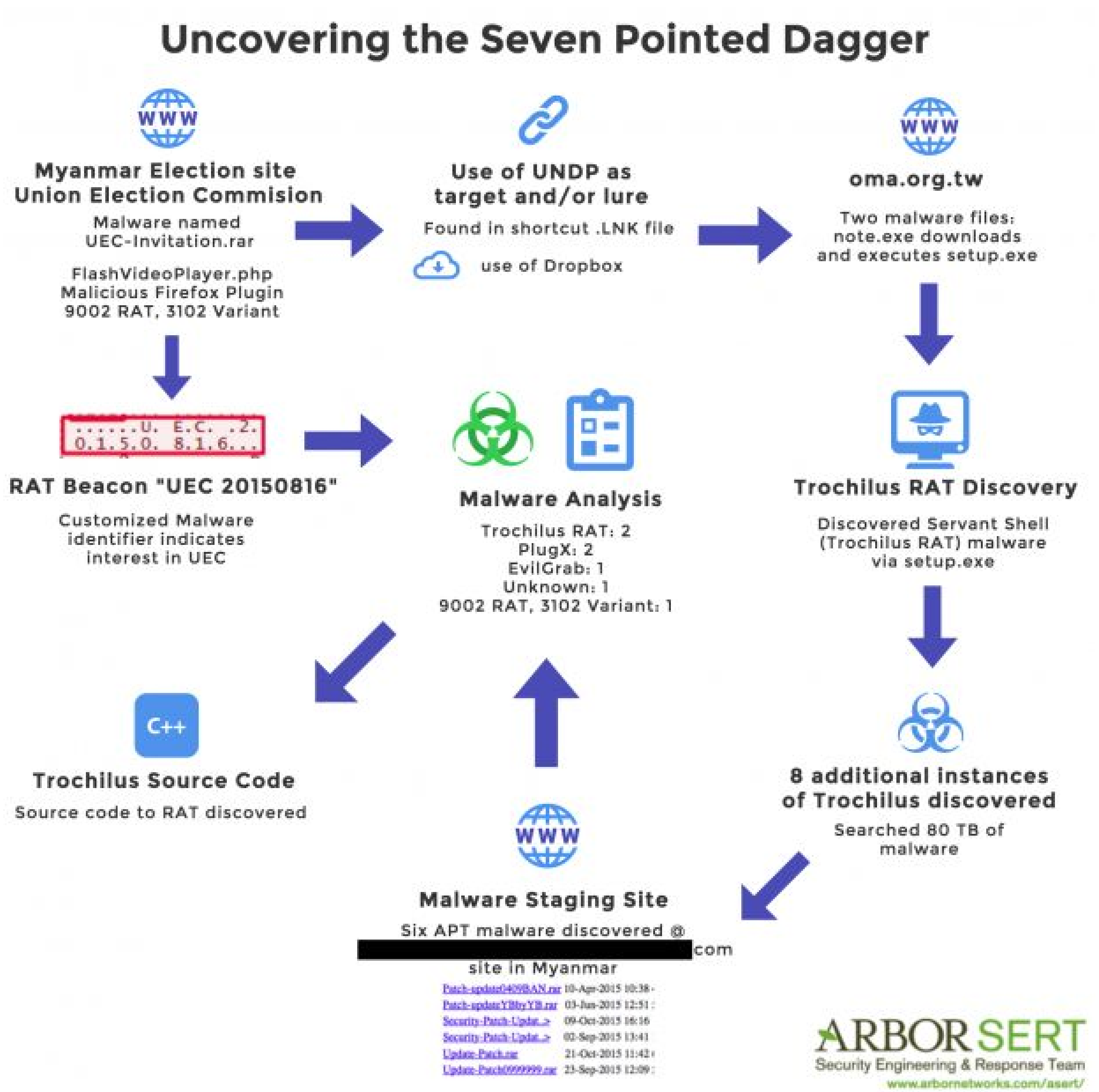
Trochilus RAT source code available on GitHub

As for Trochilus itself, Arbor's team says that the RAT has mainly reverse shell features and executes in memory only, making it very hard to detect by classic antivirus solutions. Nevertheless, some clues as to the intrusion are left behind and can be picked up by antivirus engines later on.

Furthermore, the researchers were even able to get a hold of the malware's source code, and later linked it to a GitHub profile for a user named 5loyd.

From Trochilus' GitHub project page, we see that this is "a fast&free Windows remote administration tool," coded in C++, which features support for various communications protocols, single-threaded operation, a file manager module, a remote shell, a non-UAC mode, the capability to uninstall itself, get system info from remote computers, and to download, upload, and execute files.

We doubt that 5loyd is actually part of Group 27. It may be possible that the group just hijacked his source code and used it for their malicious purposes.



Uncovering the Seven Pointed Dagger

Myanmar Election site Union Election Commision
Malware named UEC-Invitation.rar
FlashVideoPlayer.php
Malicious Firefox Plugin
9002 RAT, 3102 Variant

Use of UNDP as target and/or lure
Found in shortcut .LNK file
use of Dropbox

oma.org.tw
Two malware files: note.exe downloads and executes setup.exe

RAT Beacon "UEC 20150816"
Customized Malware identifier indicates interest in UEC

Malware Analysis
Trochilus RAT: 2
PlugX: 2
EvilGrab: 1
Unknown: 1
9002 RAT, 3102 Variant: 1

Trochilus RAT Discovery
Discovered Servant Shell (Trochilus RAT) malware via setup.exe

Trochilus Source Code
Source code to RAT discovered

8 additional instances of Trochilus discovered
Searched 80 TB of malware

Malware Staging Site
Six APT malware discovered @ [redacted]com site in Myanmar

Patch-update0409BAN.rar 10-Apr-2015 10:38
Patch-updateYBbyYB.rar 03-Jun-2015 12:51
Security-Patch-Updat..> 09-Oct-2015 16:16
Security-Patch-Updat..> 02-Sep-2015 13:41
Update-Patch.rar 21-Oct-2015 11:42
Update-Patch0999999.rar 23-Sep-2015 12:09

ARBOR SERT
Security Engineering & Response Team
www.arbornetworks.com/asert/

Seven Pointed Dagger campaign