“Red October” – Part Two, the Modules

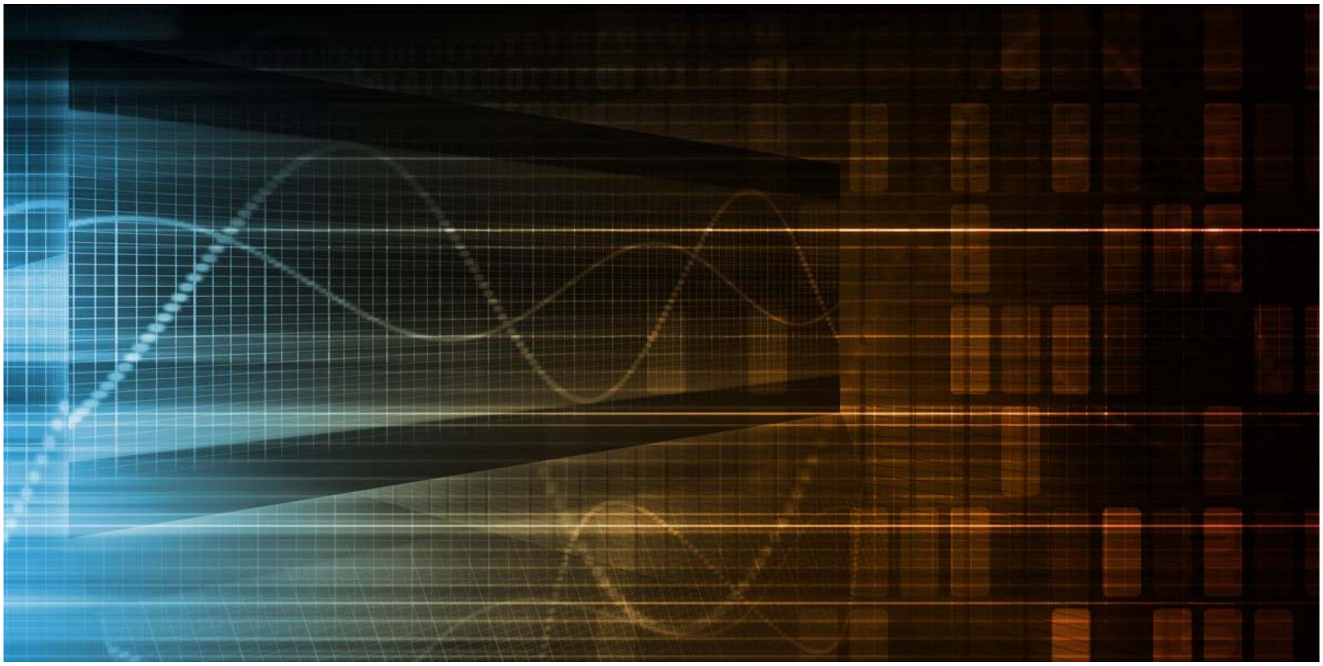
securelist.com/red-october-part-two-the-modules/57645

Incidents

Incidents

17 Jan 2013

minute read



Authors

Expert GReAT

Earlier this week, we published our report on “Red October”, a high-level cyber-espionage campaign that during the past five years has successfully infiltrated computer networks at diplomatic, governmental and scientific research organizations.

In part one, we covered the most important parts of the campaign: the anatomy of the attack, a timeline of the attacker’s operation, the geographical distribution of the victims, sinkhole information and presented a high level overview of the C&C infrastructure.

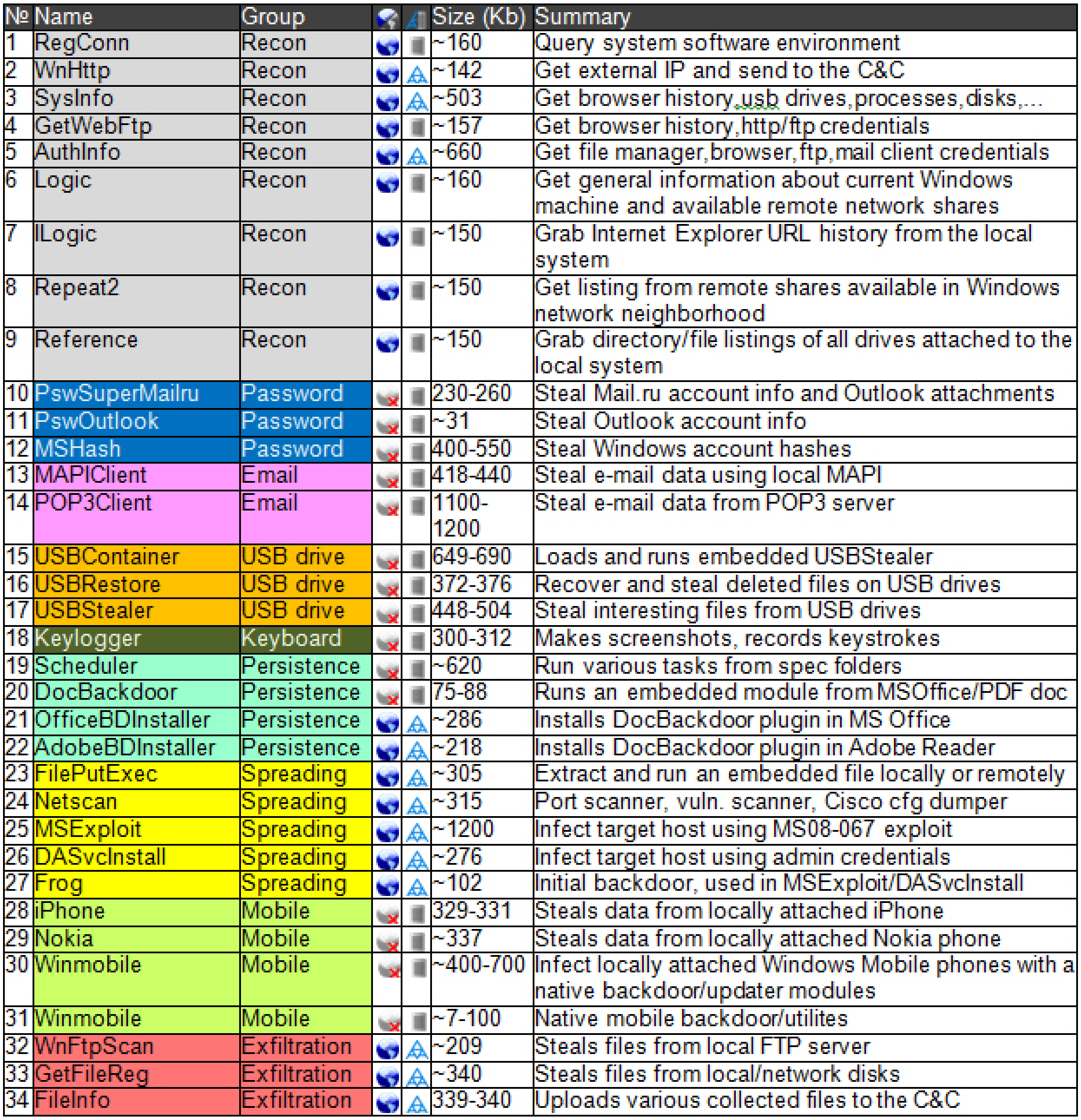
Today we are publishing part two of our research, which comprises over 140 pages of technical analysis of the modules used in the operation.

When analyzing targeted attacks, sometimes researchers focus on the superficial system infection and how that occurred. Sometimes, that is sufficient, but in the case of Kaspersky Lab, we have higher standards. This is why our philosophy is that it’s important to analyze not just the infection, but to answer three very important questions:

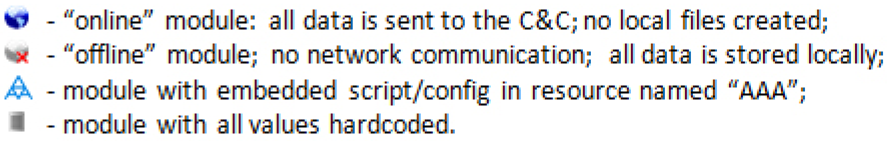
- What happens to the victim after they’re infected?
- What information is being stolen?
- Why is “Red October” such a big deal compared to other campaigns like Aurora or Night Dragon?

According to our knowledge, never before in the history of ITSec has an cyber-espionage operation been analyzed in such deep detail, with a focus on the modules used for attack and data exfiltration. In most cases, the analysis is compromised by the lack of access to the victim's data; the researchers see only some of the modules and do not understand the full purpose of the attack or what was stolen.

To get around these hiccups, we set up several fake victims around the world and monitored how the attackers handled them over the course of several months. This allowed us to collect hundreds of attack modules and tools. In addition to these, we identified many other modules used in other attacks, which allowed us to gain a unique insight into the attack.



№	Name	Group	🌐	▲	Size (Kb)	Summary
1	RegConn	Recon	🌐	▮	~160	Query system software environment
2	WnHttp	Recon	🌐	▲	~142	Get external IP and send to the C&C
3	SysInfo	Recon	🌐	▲	~503	Get browser history,usb drives,processes,disks,...
4	GetWebFtp	Recon	🌐	▮	~157	Get browser history,http/ftp credentials
5	AuthInfo	Recon	🌐	▲	~660	Get file manager,browser,ftp,mail client credentials
6	Logic	Recon	🌐	▮	~160	Get general information about current Windows machine and available remote network shares
7	ILogic	Recon	🌐	▮	~150	Grab Internet Explorer URL history from the local system
8	Repeat2	Recon	🌐	▮	~150	Get listing from remote shares available in Windows network neighborhood
9	Reference	Recon	🌐	▮	~150	Grab directory/file listings of all drives attached to the local system
10	PswSuperMailru	Password	✗	▮	230-260	Steal Mail.ru account info and Outlook attachments
11	PswOutlook	Password	✗	▮	~31	Steal Outlook account info
12	MSHash	Password	✗	▮	400-550	Steal Windows account hashes
13	MAPIClient	Email	✗	▮	418-440	Steal e-mail data using local MAPI
14	POP3Client	Email	✗	▮	1100-1200	Steal e-mail data from POP3 server
15	USBContainer	USB drive	✗	▮	649-690	Loads and runs embedded USBStealer
16	USBRestore	USB drive	✗	▮	372-376	Recover and steal deleted files on USB drives
17	USBStealer	USB drive	✗	▮	448-504	Steal interesting files from USB drives
18	Keylogger	Keyboard	✗	▮	300-312	Makes screenshots, records keystrokes
19	Scheduler	Persistence	✗	▮	~620	Run various tasks from spec folders
20	DocBackdoor	Persistence	✗	▮	75-88	Runs an embedded module from MSOffice/PDF doc
21	OfficeBDInstaller	Persistence	🌐	▲	~286	Installs DocBackdoor plugin in MS Office
22	AdobeBDInstaller	Persistence	🌐	▲	~218	Installs DocBackdoor plugin in Adobe Reader
23	FilePutExec	Spreading	🌐	▲	~305	Extract and run an embedded file locally or remotely
24	Netscan	Spreading	🌐	▲	~315	Port scanner, vuln. scanner, Cisco cfg dumper
25	MSExploit	Spreading	🌐	▲	~1200	Infect target host using MS08-067 exploit
26	DASvcInstall	Spreading	🌐	▲	~276	Infect target host using admin credentials
27	Frog	Spreading	🌐	▲	~102	Initial backdoor, used in MSExploit/DASvcInstall
28	iPhone	Mobile	✗	▮	329-331	Steals data from locally attached iPhone
29	Nokia	Mobile	✗	▮	~337	Steals data from locally attached Nokia phone
30	Winmobile	Mobile	✗	▮	~400-700	Infect locally attached Windows Mobile phones with a native backdoor/updater modules
31	Winmobile	Mobile	✗	▮	~7-100	Native mobile backdoor/utilites
32	WnFtpScan	Exfiltration	🌐	▲	~209	Steals files from local FTP server
33	GetFileReg	Exfiltration	🌐	▲	~340	Steals files from local/network disks
34	FileInfo	Exfiltration	🌐	▲	339-340	Uploads various collected files to the C&C



🌐 - "online" module: all data is sent to the C&C; no local files created;
✗ - "offline" module; no network communication; all data is stored locally;
▲ - module with embedded script/config in resource named "AAA";
▮ - module with all values hardcoded.

The research that we are publishing today is perhaps the biggest malware research paper ever. It is certainly the most complex malware research effort in the history of our company and we hope that it sets new standards for what anti-virus and anti-malware research means today.

Because of its size, we've split "part 2" in several pieces, to make reading easier:

First stage of attack

Second stage of attack

- Malware Descriptions
- Microsoft
- Microsoft Windows
- Mobile Malware
- Spear phishing
- Targeted attacks

Authors

Expert GReAT

“Red October” – Part Two, the Modules

26 Feb 2021, 12:00pm
17 Jun 2020, 1:00pm
26 Aug 2020, 2:00pm
22 Jul 2020, 2:00pm
From the same authors

APT trends report Q2 2021

Arrests of members of Tetrade seed groups Grandoreiro and Melcoz

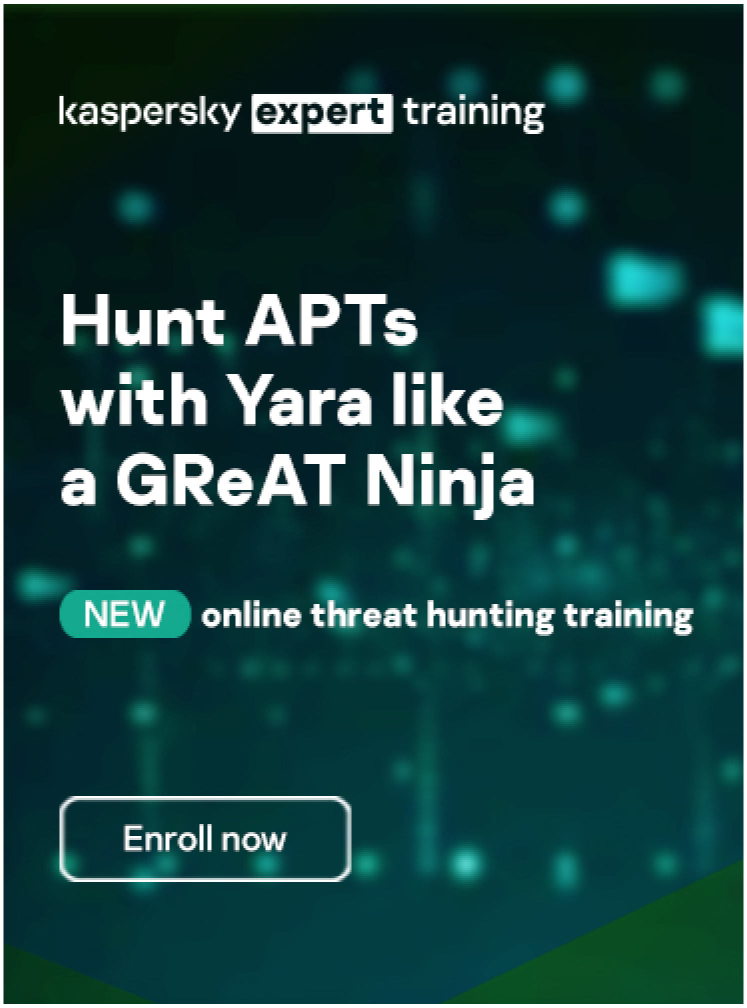
Ferocious Kitten: 6 years of covert surveillance in Iran

Bizarro banking Trojan expands its attacks to Europe

APT trends report Q1 2021

-
-
-

-


kaspersky expert training
Hunt APTs with Yara like a GReAT Ninja
NEW online threat hunting training
Enroll now

Reports

Kimsuky’s GoldDragon cluster and its C2 operations

Kimsuky (also known as Thallium, Black Banshee and Velvet Chollima) is a prolific and active threat actor primarily targeting Korea-related entities. In early 2022, we observed this group was attacking the media and a think-tank in South Korea.

VileRAT: DeathStalker’s continuous strike at foreign and cryptocurrency exchanges

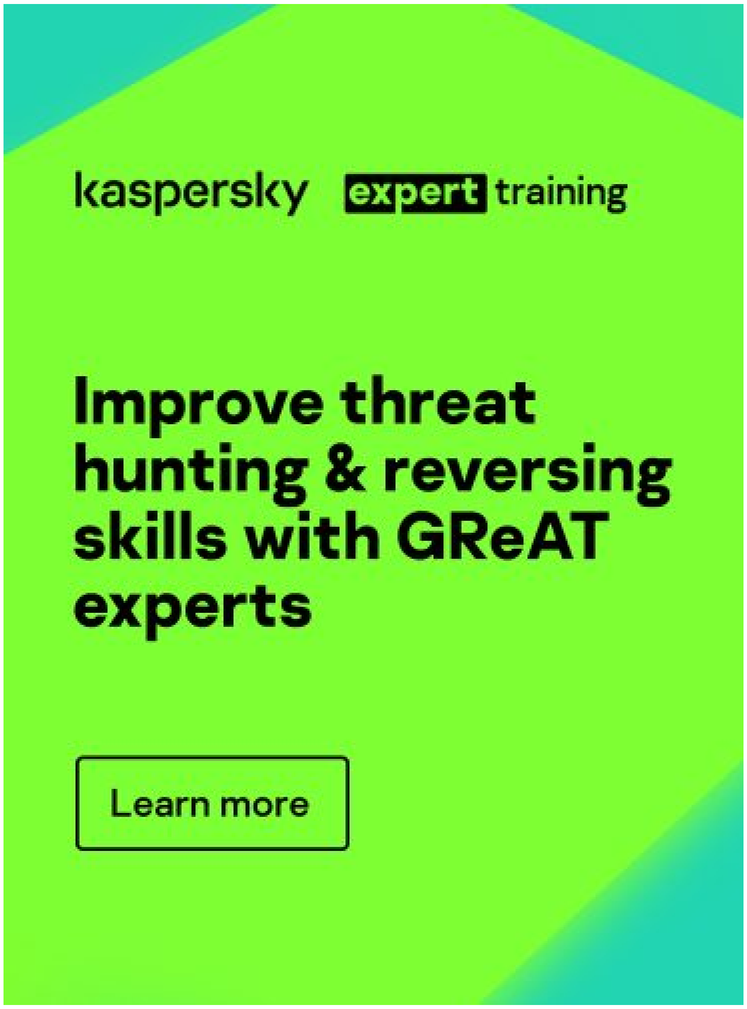
VileRAT is a Python implant, part of an evasive and highly intricate attack campaign against foreign exchange and cryptocurrency trading companies.

Andariel deploys DTrack and Maui ransomware

Earlier, the CISA published an alert related to a Stairwell report, “Maui Ransomware.” Our data should openly help solidify the attribution of the Maui ransomware incident to the Korean-speaking APT Andariel, also known as Silent Chollima and Stonefly.

Targeted attack on industrial enterprises and public institutions

Kaspersky ICS CERT experts detected a wave of targeted attacks in several East European countries, as well as Afghanistan. Of the six backdoors identified on infected systems, five have been used earlier in attacks attributed to APT TA428.


kaspersky
expert training
Improve threat hunting & reversing skills with GReaT experts
Learn more

Subscribe to our weekly e-mails

The hottest research right in your inbox

-
-
-