Threatpost

- **Categories**
  - **Category List**
    - Apple
    - Cloud Security
    - Compliance
    - Critical Infrastructure
    - Cryptography
    - Government
  - **Category List**
    - Hacks
    - Malware
    - Microsoft
    - Mobile Security
    - Privacy
  - **Category List**
    - SMB Security
    - Social Engineering
    - Virtualization
    - Vulnerabilities
    - Web Security
- **Authors**
  - Dennis Fisher
  - Michael Mimoso
  - Christopher Brook
  - Brian Donohue
  - Anne Saita
- **Additional Categories**
  - Slideshows
- **The Kaspersky Lab News Service**
- **Featured**
  - **Authors**
    - Dennis Fisher
Featured Posts

All

Picture-Based Password Schemes Have Their Weaknesses

Public Exploit Available for Patched Safari...

Njw0rm: A RAT With Legs and...

Podcasts

Latest Podcasts

All

Threatpost News Wrap, August 30, 2013

How I Got Here: Jeremiah Grossman
How I Got Here: Rich Mogull

Joe Grand on Hardware Hacking and...

Threatpost News Wrap, August 9, 2013

Matthew Green on Crypto Advances, the...

Recommended

- How I Got Here: Jeremiah Grossman
- Chris Soghoian on the NSA Surveillance and Government Hacking
- Adrian Stone on BlackBerry Security, Privacy and the Challenges of BYOD
- Anup Ghosh on Cyberespionage, Attribution and APTs

The Kaspersky Lab Security News Service

- Videos

Latest Videos

All

Jeff Forristal on the Android Master-Key...

Researchers Discover Dozens of Gaming Client...
Recommended

- Lock Screen Bypass Flaw Found in Samsung Androids
- Facebook Patches OAuth Authentication Vulnerability
- Video: Locking Down iOS

The Kaspersky Lab Security News Service

Twitter
Facebook
Google
LinkedIn
YouTube
RSS

09/05/13 7:20
Watch-Like Heartbeat Monitor Seeks to Replace #Passwords with Electrocardiograms - http://t.co/JwMpN6zn0Y
NetTraveler Variant Adds Java Exploits, Watering Hole Attacks to Bag of Tricks
When NetTravler was unveiled in June, Costin Raiu of Kaspersky Lab warned that the espionage campaign was an “ugly gorilla with a thousand faces” and that we hadn’t seen them all yet.

A little more than two months later, another profile of the malware targeting activists, diplomats, government targets and the scientific research community, has reared its head.

Related Posts

Java’s Losing Security Legacy

September 4, 2013, 5:26 pm

Njw0rm: A RAT With Legs and a Thirst for No-IP Credentials

September 3, 2013, 3:29 pm

Java 6 Zero Day a Reminder to Upgrade Browser Plug-In

August 28, 2013, 12:44 pm

Raiu said today that a variant has been spotted by Kaspersky’s Global Research and Analysis Team and unlike its first go-round which targeted Microsoft Office vulnerabilities, this new take on NetTraveler exploits a recently patched Java bug. The group behind the attacks has also jumped on the watering hole attack bandwagon, having compromised an Uyghur-related website and redirecting victims to an attack site.

“Watering hole attacks have become another popular method to attack unsuspecting victims by the APT operators,” Raiu wrote on Securelist, the Kaspersky Lab research blog. “There is perhaps no surprise that the NetTraveler attacks are now using this method as well.”

NetTraveler has zeroed in on Tibetan and Uyghur activists in addition to a number of manufacturing, research and even military targets. The first version, which spread via spear phishing emails and dropped Office documents carrying malicious attachments, exfiltrated files from victims’ machines and send them to a command and control infrastructure that overlapped with one used by the Gh0st RAT campaign. Office document files such as Word, Excel and PowerPoint files were uploaded to command and control servers; the malware’s
configuration files can also be modified to steal design documents such as those done on Corel Draw or AutoCAD files. To date, NetTraveler has infected victims in more than 40 countries, Raiu said.

The variant reported today also targets the same victim demographics, but has expanded beyond spear phishing to watering hole attacks, which provide attackers with the ability to cast a wider net at potential victims by infecting websites they’re likely to visit with exploits that redirect them to an attacker-controlled site where more malware awaits.

The updated NetTraveler was spotted in the last week, Raiu said, targeting several Uyghur activists with an email promising a statement from the World Uyghur Congress on a massacre in the Karghiliq country. The link to the statement spoofs the Uyghur Congress website, and instead points victims to a NetTraveler domain weststock[.]org. A Java exploit called new.jar on the page is for a vulnerability patched in June by Oracle, CVE-2013-2465, that affects Java 7U21 and earlier, Java 6U45 and earlier and Java 5U45 and earlier. The payload is a backdoor dropper called file.temp used by NetTraveler, compiled on May 30, Raiu said.

Once up and running on the victim’s machine, the NetTraveler variant connects to a command and control server hosted at Multacom Corp., in Los Angeles; the IP address is 198[.]211[.]18[.]93. Raiu said that the command server is still operational and that the server exclusively hosts the attack server.

Meanwhile, the NetTraveler group has also apparently compromised a Uyghur-related website at the Islamic Association of Eastern Turkistan with an iframe attack that redirects victims to the weststock[.]org domain.

“The usage of the Java exploit for CVE-2013-2465 coupled with the watering hole attacks is a new, previously unseen development for the NetTraveler group,” Raiu said. “It obviously has a higher success rate than mailing CVE-2012-0158 exploit-ridden documents, which was the favorite attack vector until now. We estimate that more recent exploits will be integrated and used against the group’s targets.”

Neither NetTraveler iteration relied on zero days, Raiu said. The first version of NetTraveler targeted Office vulnerabilities that had been patched almost a year, yet still Kaspersky Lab researchers were able to find more than 22 gigabytes of stolen data on sinkholed command and control servers—a small fraction of the stolen data. More than 30 command and control servers have been discovered between the two versions of the campaign.
Java’s Losing Security Legacy

by Michael Mimoso

Java’s code-signing requirements have proven to be a bust, security researchers say, and now even longtime developers are losing faith in the programming language.

Read more...
Njw0rm: A RAT With Legs and a Thirst for No-IP Credentials

by Michael Mimoso

The njw0rm, an offshoot of njRAT, is espionage malware like its forerunner, but also has the ability to spread via removable storage devices, as well as steal No-IP credentials.

Read more...

Java 6 Zero Day a Reminder to Upgrade Browser Plug-In

by Chris Brook
Java users get another reminder to upgrade to current versions of the browser plug-in after a zero day targeting a previously patched Java 6 bug was found in the Neutrino Exploit Kit

Read more...

Top Stories

Java’s Losing Security Legacy
September 4, 2013, 5:26 pm

How I Got Here: Jeremiah Grossman
August 27, 2013, 10:30 am

Facebook Produces First Report on Government Requests for Data
August 27, 2013, 2:54 pm

DHS Warns Fire, Police Departments About Android Threats
August 27, 2013, 2:07 pm

Updated Drive/DirtJumper DDoS Toolkit Includes Mitigation Bypasses
August 27, 2013, 1:41 pm

Ubuntu Forums Remain Down After Password Breach
July 22, 2013, 11:07 am

Threatpost News Wrap, August 30, 2013
August 30, 2013, 9:20 am
Cisco Warns Users of Four Vulnerabilities

September 3, 2013, 2:46 pm

Tortilla Tool Anonymously Routes TCP, DNS Traffic Through Tor

July 15, 2013, 12:58 pm

The Final Say

From Kaspersky Blogs

Deutsche QR hotel....

Guten tag folks! I’m currently on a trans-Europe express road trip. And along the way I keep coming across such unusual sights that I feel I’m simply duty-bound to share them with the world’s more pro...

Read more...

I’ve had the great opportunity to present at the Nordic Security Conference. This year I gave a presentation about one of the weakest links in IT-security; the human factor.

Read more...

Gamescom – A Paradise For Gamer Geeks...

Record number of visitors at Gamescom this year Last week, the world’s largest gaming convention, Gamescom, took place in Cologne for the third year running. The many innovations and exclusive preview...

Read more...
Apple Developer Center down for a week

It took Apple about a week to restore the functions of the Apple Developer Center following its crash on July 18. After about three days, Apple officially acknowled...