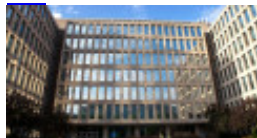
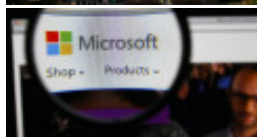


Threatpost | The first stop for security news

- [Categories](#)
 - [Category List](#)
 - [Apple](#)
 - [Cloud Security](#)
 - [Compliance](#)
 - [Critical Infrastructure](#)
 - [Cryptography](#)
 - [Government](#)
 - [Category List](#)
 - [Hacks](#)
 - [Malware](#)
 - [Microsoft](#)
 - [Mobile Security](#)
 - [Privacy](#)
 - [Ransomware](#)
 - [Category List](#)
 - [SAS](#)
 - [SMB Security](#)
 - [Social Engineering](#)
 - [Virtualization](#)
 - [Vulnerabilities](#)
 - [Web Security](#)
 - [Authors](#)
 - [Michael Mimoso](#)
 - [Christopher Brook](#)
 - [Additional Categories](#)
 - [Slideshows](#)
 - [The Kaspersky Lab News Service](#)
- [Featured](#)
 - [Authors](#)
 - [Michael Mimoso](#)
 - [Christopher Brook](#)
 - [The Kaspersky Lab News Service](#)

Featured Posts

[All](#)[5.6 Million Fingerprints Stolen In OPM...](#)[Bypass Developed for Microsoft Memory Protection,...](#)[Federal CISOs Propose New Efforts to...](#)

- [Podcasts](#)

Latest Podcasts

[All](#)



[Dennis Fisher On Security, Journalism, and...](#)



[Gary McGraw on Scalable Software Security...](#)



[Threatpost News Wrap, September 4, 2015](#)

[How I Got Here: Window Snyder](#)

[Threatpost News Wrap, August 28, 2015](#)

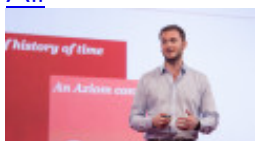
[Threatpost News Wrap, August 14, 2015](#)

Recommended

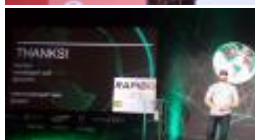
- [Robert Hansen on Aviator, Search Revenue and the \\$250,000 Security Guarantee](#)
- [Threatpost News Wrap, February 21, 2014](#)
- [How I Got Here: Jeremiah Grossman](#)
- [Chris Soghoian on the NSA Surveillance and Government Hacking](#)
- [The Kaspersky Lab Security News Service Videos](#)

Latest Videos

[All](#)



[Kris McConkey on Hacker OpSec Failures](#)



[Trey Ford on Mapping the Internet...](#)



[Christofer Hoff on Mixed Martial Arts,...](#)



[Twitter Security and Privacy Settings You...](#)



[The Biggest Security Stories of 2013](#)

[Jeff Forristal on the Android Master-Key...](#)

Recommended

- [Twitter Security and Privacy Settings You Need to Know](#)
- [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](#)

09/25/15 4:27

FYI--had a commenting issue on the site for a few days this week - but it should be fixed now.

-
-

[Welcome](#) > [Blog Home](#) > [Critical Infrastructure](#) > Naikon APT Group Tied to China' s PLA Unit 78020



Naikon APT Group Tied to China' s PLA Unit 78020

 Follow @mike_mimoso by [Michael Mimoso](#) September 24, 2015 , 1:37 pm

Chinese president Xi Jinping is supposed to have dinner this evening with U.S. president Barack Obama. Wonder if the name Ge Xing will come up?

Ge Xing is the subject of a joint [report](#) published this morning by ThreatConnect and Defense Group Inc., computer and national security service providers respectively. Ge is alleged to be a member of the People's Liberation Army unit 78020, a state-sponsored hacking team whose mission is to collect intelligence from political and military sources to advance China's interests in the South China Sea, a key strategic and economic region in Asia with plenty of ties to the U.S.

Related Posts

[XcodeGhost Malware Stirring Up More Trouble](#)

September 23, 2015 , 9:37 am

[XcodeGhost iOS Malware Contained](#)

September 21, 2015 , 1:00 pm

[Turla APT Group Abusing Satellite Internet Links](#)

September 9, 2015 , 9:00 am

The report connects PLA 78020 to the Naikon advanced persistent threat group, a state-sponsored outfit that has followed the APT playbook to the letter to infiltrate and steal sensitive data and intellectual property from military, diplomatic and enterprise targets in a number of Asian countries, as well as the United Nations Development Programme and the Association of Southeast Asian Nations (ASEAN).

Control over the South China Sea is a focal point for China; through this region flows trillions of dollars of commerce and China has not been shy about claiming its share of the territory. The report states that China uses its offensive hacking capabilities to gather intelligence on adversaries' military and diplomatic intentions in the regions, and has leveraged the information to strengthen its position.

"The South China Sea is seen as a key geopolitical area for China," said Dan Alderman, deputy director of DGI. "With Naikon, we see their activity as a big element of a larger emphasis on the region and the Technical Reconnaissance Bureau fitting into a multisector effort to influence that region."

The report is just the latest chess piece hovering over Jinping's U.S. visit this week, which began in earnest yesterday with a visit to Seattle and meetings with giant technology firms such as Microsoft, Apple and Google, among others. Those companies want to tap into the growing Chinese technology market and the government there is using its leverage to get them to support stringent Internet controls imposed by the Chinese government.

A letter sent to American technology companies this summer, a [New York Times](#) report last week, said that China would ask American firms to store Chinese user data in China. China also reportedly asked U.S.-built software and devices sold in China to be "secure and controllable," which likely means the Chinese would want backdoor access to these products, or access to private encryption keys.

Jinping, meanwhile, tried to distance himself from the fray when he said in a *Wall Street Journal* interview: "Cyber theft of commercial secrets and hacking attacks against government networks are both illegal; such acts are criminal offences and should be punished according to law and relevant international conventions."

Journal reporter [Josh Chin connected with Ge Xing over the phone](#) and Ge confirmed a number of the dots connected in the report before hanging up on the reporter and threatening to report him to the police. While that never happened, the infrastructure connected to Ge and this slice of the Naikon APT group, was quickly shut down and taken offline.

In May, researchers at Kaspersky Lab published a report on [Naikon](#) and documented five years of activity attributed to the APT group. It describes a high volume of [geo-politically motivated attacks](#) with a high rate of success infiltrating influential organizations in the region. The group uses advanced hacking tools, most of which were developed externally and include a full-featured backdoor and exploit builder.

Like most APT groups, they craft tailored spear phishing messages to infiltrate organizations, in this case a Word or Office document carrying an exploit for CVE-2012-0158, a favorite target for APT groups. The vulnerability is a buffer overflow in the ActiveX controls of a Windows library, MSCOMCTL.OCX. The exploit installs a remote administration tool, or RAT, on the compromised machine that opens a backdoor through which stolen data is moved out and additional malware and instructions can be moved in.

Chin's article describes a similar attack initiated by Ge, who is portrayed not only as a soldier, but as an academic. The researchers determined through a variety of avenues that Ge is an active member of the military, having published research as a member of the military, in addition to numerous postings to social media as an officer and via his access to secure locations believed to be headquarters to the PLA unit's technical reconnaissance bureau.

"Doing this kind of biopsy, if you will, of this threat through direct analysis of the technical and non-technical evidence allows us to paint a picture of the rest of this group's activity," said Rich Barger, CIO and cofounder of ThreatConnect. "We've had hundreds of hashes, hundreds of domains, and thousands of IPs [related to PLA unit 78020]. Only looking at this from a technical lens only gives you so much. When you bring in a regional, cultural and even language aspect to it, you can derive more context that gets folded over and over into the technical findings and continues to refine additional meaning that we can apply to the broader group itself."

The report also highlights a number of operational security mistakes Ge made to inadvertently give himself away, such as using the same handle within the group's infrastructure, even embedding certain names in families of malware attributed to them. All of this combined with similar mistakes made across the command and control infrastructure and evidence pulled from posts on social media proved to be enough to tie Ge to the Naikon group and elite PLA unit that is making gains in the region.

"If you look at where China is and how assertive they are in region, it might be a reflection of some of the gains and wins this group has made," Barger said. "You don't influence what they're influencing in the region if you don't have the intel support capabilities fueling that operational machine."



Categories: [Critical Infrastructure](#), [Government](#), [Hacks](#), [Malware](#)

Leave A Comment

Your email address will not be published. Required fields are marked *


Name

Email

Comment

You may use these HTML tags and attributes: <abbr title=""> <acronym title=""> <blockquote cite=""> <cite> <code> <del datetime=""> <i> <q cite=""> <s> <strike>

☐ I'm not a robot


reCAPTCHA
[Privacy](#) - [Terms](#)

Post Comment

- ☐ Notify me of follow-up comments by email.
- ☐ Notify me of new posts by email.

Recommended Reads



September 23, 2015 , 9:37 am

Categories: [Apple](#), [Malware](#), [Vulnerabilities](#)

[XcodeGhost Malware Stirring Up More Trouble](#)

by [Michael Mimoso](#)

Researchers found a weakness in XcodeGhost that puts it at risk for man-in-the-middle attacks.

[Read more...](#)



September 21, 2015 , 1:00 pm

Categories: [Apple](#), [Malware](#), [Mobile Security](#)

[XcodeGhost iOS Malware Contained](#)

by [Michael Mimoso](#)

iOS apps infected with the XcodeGhost malware have been removed from the App Store and three command domains communicating with infected apps have been shut down.

[Read more...](#)



September 9, 2015 , 9:00 am

Categories: [Critical Infrastructure](#), [Hacks](#), [Malware](#), [Vulnerabilities](#), [Web Security](#)

[Turla APT Group Abusing Satellite Internet Links](#)

by [Michael Mimoso](#)

Researchers at Kaspersky Lab have revealed that the Turla APT gang is using satellite-based Internet links to hide command-and-control activities.

[Read more...](#)

Top Stories

[XcodeGhost Malware Stirring Up More Trouble](#)

September 23, 2015 , 9:37 am

[Stagefright Patch Incomplete Leaving Android Devices Still Exposed](#)

August 13, 2015 , 1:00 pm

[Unusual Re-Do of US Wassenaar Rules Applauded](#)

July 31, 2015 , 12:56 pm

[Emergency IE Patch Fixes Vulnerability Under Attack](#)

August 18, 2015 , 6:08 pm

[KeyRaider Malware Steals Certificates, Keys and Account Data From Jailbroken iPhones](#)

August 31, 2015 , 9:09 am

[Writing Advanced OS X Malware an 'Elegant' Solution to Improving Detection](#)

July 30, 2015 , 1:56 pm

[Risky Schneider Electric SCADA Vulnerabilities Remain Unpatched](#)

August 17, 2015 , 3:11 pm

[APT Group Gets Selective About Data it Steals](#)

August 5, 2015 , 3:00 pm

[Researchers Outline Vulnerabilities in Yahoo, PayPal, Magento Apps](#)

September 11, 2015 , 1:07 pm

TIP #3



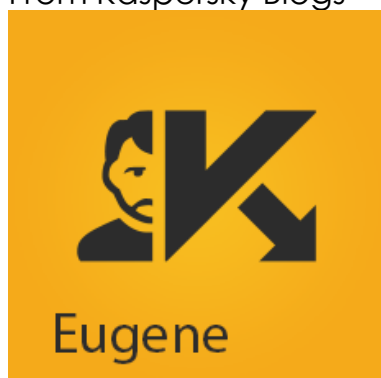
**Security policies
should work
everywhere**

even outside the workplace

[Click to learn more](#)

The Final Say

From Kaspersky Blogs



[Kamchatka-2015: Ksudach – the Countach of the volc...](#)

The Ksudach volcano is one of the most unusual and breathtakingly beautiful places on our planet – I assure you. And since I’ m lucky enough to have been practically everywhere on the planet, my ...

[Read more...](#)



[Coinvault, are we reaching the end of the nightmar...](#)

After obtaining the new MD5 hashes for the CoinVault files, we set out to find more clues, more files, and to analyse what these new malware variants had to reveal. However, the best thing was that, b...

[Read more...](#)



[Pitting wits with a tablet: 10 best mobile games f...](#)

Despite our dismay about too much computer in our kids’ lives, it’ s a process, which cannot be stopped now. Since we cannot stop it, let’ s steer it in the right direction!...

[Read more...](#)



[Hacking-Back: Six Justifications for Doing It and ...](#)

If the idea of “hacking-back” against cybercriminals who have harmed you or your company has seized you, your executive team, or your spouse as a reasonable thing to do, read on. It’ ...

[Read more...](#)



[Encryption...](#)

Ignoring the safety of information stored on our computers and removable devices means putting that information at risk. Sooner or later someone will be interested in knowing whether you store your cr...

[Read more...](#)

[Threatpost](#) | [The first stop for security news](#) The Kaspersky Lab Security News Service
Categories [Apple](#) | [Black Hat](#) | [Cloud Security](#) | [Compliance](#) | [Critical Infrastructure](#) |
[Cryptography](#) | [Data Breaches](#) | [Featured](#) | [Featured Podcast](#) | [Featured Video](#) |
[Google](#) | [Government](#) | [Hacks](#) | [How I Got Here](#) | [Malware](#) | [Microsoft](#) | [Mobile Security](#)
| [Podcasts](#) | [Privacy](#) | [Ransomware](#) | [Scams](#) | [Security Analyst Summit](#) | [Slideshow](#) | [SMB](#)
[Security](#) | [Social Engineering](#) | [Uncategorized](#) | [Videos](#) | [Virtualization](#) | [Vulnerabilities](#) |
[Web Security](#)

- [RSS Feeds](#)
- [Home](#)
- [About Us](#)
- [Contact Us](#)

Authors

[Michael Mimoso](#)
[Christopher Brook](#)

Copyright © 2015 [Threatpost](#) | [The first stop for security news](#)

- | [Terms of Service](#)
- | [Privacy](#)