informa

InformationWeek IT NETWORK | Dark Reading | Network Computing | About Us | Advertise | Register | Login to your account | Welcome Guest

DARKReading | SIGN UP FOR OUR NEWSLETTERS | Search Dark Reading

Authors | Slideshows | Video | Tech Library | University | Radio | Calendar | Black Hat News | Follow DR:

THE EDGE | ANALYTICS | ATTACKS / BREACHES | APP SEC | CAREERS & PEOPLE | CLOUD | ENDPOINT | IoT | OPERATIONS | PERIMETER | RISK | THREAT INTELLIGENCE | VULNS / THREATS

THREAT INTELLIGENCE

3/1/2016
04:21 AM

Sara Peters
News

Connect Directly

0 COMMENTS
COMMENT NOW

Login
50% 50%

Like | Tweet | Share

Chinese Threat Intel Start-up Finds DarkHotel Exploiting Chinese Telecom

New China-based threat intelligence company ThreatBook wants to be the 'trusted contact in China.'

SAN FRANCISCO, RSA Conference -- The DarkHotel threat group is targeting executives at telecommunications companies in North Korea and China, already compromising at least one, according to researchers at Beijing-based threat intelligence start-up ThreatBook.

In operation since 2007, DarkHotel is named for their habit of exploiting executives while they were using unsecured hotel WiFi networks, a behavior the group has since abandoned. In this campaign, which ThreatBook refers to as DarkHotel Operation 8651, the group is using spearphishing messages with malicious documents attached -- specifically, a crafted SWF file embedded as a downloadable link in a Word document.

The SWF file exploits Adobe Flash vulnerability CVE-2015-8651. According to ThreatBook, the earliest infections associated with that bug and this campaign are Dec. 24. Adobe released an out-of-band patch for it Dec. 28.

The payload, update.exe, is a Trojan downloader, disguised as a component of OpenSSL. It then uses a variety of anti-detection measures, including anti-sandbox, and anti-anti-virus, as well as just-in-time decryption.

Feng Xue and Hong Jia, friends from their days working at Microsoft, first had the idea to start ThreatBook in May. After a hurried meeting at the Beijing airport Starbucks during Jia's two-hour layover en route to Redmond, Wash., the two quit their jobs -- Jia as principal anti-virus research manager at Microsoft and Feng as CISO of Amazon.cn -- and launched ThreatBook in June.

"I never thought I would leave [Microsoft]," says Jia. "The career path was quite good and I love Microsoft."

"I got excited and I could not sleep," says Xue.

The idea that hooked Xue and Jia was realizing that there was no threat intelligence market in China, but the need for one was great.

"Threat intelligence is not just a tool, it's a new wave. A trend," says Xue.

ThreatBook uncovered information about the identity and intentions of the XCodeGhost authors in October. This week they are exhibiting at RSA, introducing their security threat analysis platform and Threat Intelligence Center.

Xue says that at previous positions he's held there was a lack of understanding of China's unique landscape. He'd have to spend some of time at old jobs educating colleagues about, for example, enormous cybersecurity incidents in China that are so underreported in the West that they aren't even mentioned in yearly wrap-ups of top global attacks. "I feel sometimes frustrated," Xue says.

Jia says this is one of the things she wants ThreatBook to be able to fix. She says their focus is China-focused threat intelligence, and they're very open to exchanging information with other companies and other organizations.

"Our company is a bridge," she says. "We want to be the trusted contact in China."

Related Content:

- **Cybercrime And Hacking Atlas (China)**
- **Sony Hackers Behind Previous Cyberattacks Tied To North Korea**
- **Sony Hackers Still Active, 'Darkhotel' Checks Out Of Hotel Hacking**

Interop Las Vegas

Find out more about security threats at Interop 2016, May 2-6, at the Mandalay Bay Convention Center, Las Vegas. Register today and receive an early bird discount of $200.

Sara Peters is Senior Editor at Dark Reading and formerly the editor-in-chief of Enterprise Efficiency. Prior that she was senior editor for the Computer Security Institute, writing and speaking about virtualization, identity management, cybersecurity law, and a myriad ... View Full Bio

COMMENT | EMAIL THIS | PRINT | RSS

MORE INSIGHTS

Webcasts
- Chatbots for the Enterprise
- Security Alert Fatigue: Tips for Taking Control

MORE WEBCASTS

White Papers
- 2020 IT Salary Survey Results Revealed
- NetFlow vs Packet Data

MORE WHITE PAPERS

Reports
- 2020 IT Salary Survey Results Revealed
- [Report] DevSecOps & Secure App Delivery: What's Working & What's Not

MORE REPORTS

COMMENTS

NEWEST FIRST | OLDEST FIRST | THREADED VIEW

Be the first to post a comment regarding this story.

HOT TOPICS | EDITORS' CHOICE

Many Ransomware Attacks Can be Stopped Before They Begin
Jai Vijayan, Contributing Writer, 3/17/2020 — 2

Why CSP Isn't Enough to Stop Magecart-Like Attacks
Hadar Blutrich, CTO & Co-founder, Source Defense, 3/11/2020 — 1

How the Rise of IoT Is Changing the CISO Role
Phil Neray, VP of IoT & Industrial Cybersecurity at CyberX, 3/11/2020 — 1

NEWS | SUBSCRIBE TO NEWSLETTERS

WEBINARS

Building an Enterprise Strategy for Detection and Response (XDR)

Chatbots for the Enterprise

5 Steps to Integrate SAST into the DevSecOps Pipeline

WEBINAR ARCHIVES

WHITE PAPERS

- 2020 IT Salary Survey Results Revealed
- NetFlow vs Packet Data
- Global Application and Network Security Report
- Research Report: Evaluating Your Organization's Cybersecurity Readiness
- How to Pick a Winner in EDR

MORE WHITE PAPERS

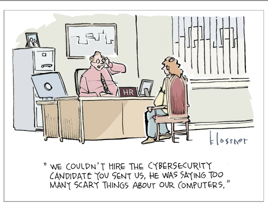
VIDEO

Ransomware Trains Its Sights on Cloud ...
6 COMMENTS

Qualys Launches Free App for IT Asset ...
1 COMMENTS

ALL VIDEOS

CARTOON



"WE COULDN'T HIRE THE CYBERSECURITY CANDIDATE YOU SENT US, HE WAS SAYING TOO MANY SCARY THINGS ABOUT OUR COMPUTERS."

Latest Comment: Unfortunately nobody wants to spend money on security. Usually they change their mind but often it is too late

CARTOON ARCHIVE

CURRENT ISSUE

6 Emerging Cyber Threats That Enterprises Face in 2020

This Tech Digest gives an in-depth look at six emerging cyber threats that enterprises could face in 2020. Download your copy today!

DOWNLOAD THIS ISSUE!

BACK ISSUES | MUST READS

FLASH POLL

Has the U.S. political climate caused you to make infosecurity-related changes to your disaster recovery/business continuity plans?

○ Yes

○ No

○ No but we are considering it

○ Still waiting for cybersecurity guidance from Trump admin EO

○ Don't know

○ Other (Please explain in the comments)

Submit

ALL POLLS

REPORTS

State of Cybersecurity Incident Response

Data breaches and regulations have forced organizations to pay closer attention to the security incident response function. However, security leaders may be overestimating their ability to detect and respond to security incidents. Read this report to find out more.

DOWNLOAD NOW!

How Enterprises Are Developing and Maintaining Secure Applications — 0 COMMENTS

How Enterprises are Attacking the Cybersecurity Problem — 0 COMMENTS

How Data Breaches affect the Enterprise — 0 COMMENTS

MORE REPORTS

TWITTER FEED

BUG REPORT

ENTERPRISE VULNERABILITIES
From DHS/US-CERT's National Vulnerability Database

- **CVE-2020-3922**
  PUBLISHED: 2020-03-18
  LisoMail, by ArmorX, allows SQL Injections, attackers can access the database without authentication via a URL parameter manipulation.
- **CVE-2020-10659**
  PUBLISHED: 2020-03-18
  Entrust Entelligence Security Provider (ESP) before 10.0.60 on Windows mishandles errors during SSL Certificate Validation, leading to situations where (for example) a user continues to interact with a web site that has an invalid certificate chain.
- **CVE-2020-8468**
  PUBLISHED: 2020-03-18
  Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) agents are affected by a content validation escape vulnerability which could allow an attacker to manipulate certain agent client components. An attempted attack requires user authentication.
- **CVE-2020-8470**
  PUBLISHED: 2020-03-18
  Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) server contains a vulnerable service DLL file that could allow an attacker to delete any file on the server with SYSTEM level privileges. Authentication is not required to exploit this vulnerability.
- **CVE-2020-8598**
  PUBLISHED: 2020-03-18
  Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) server contains a vulnerable service DLL file that could allow a remote attacker to execute arbitrary code on affected installations with SYSTEM level privileges. Authentication is not required to exploit th...