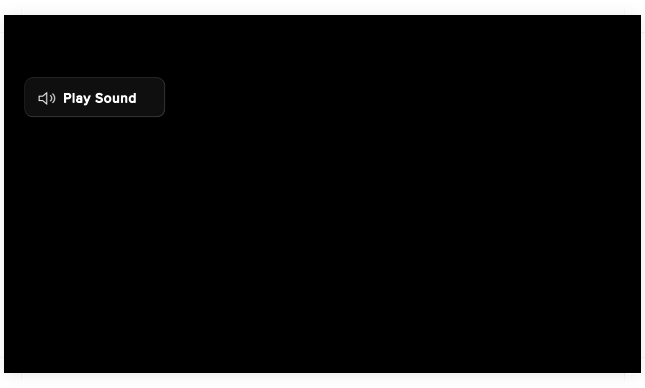
MUST READ: Intel is teaching a computer chip to smell

Internet Explorer scripting engine becomes North Korean APT's favorite target in 2018

North Korean hacking group focuses attacks on aging and soon-to-be-deprecated technology.

By Catalin Cimpanu for Zero Day | November 12, 2018 -- 19:29 GMT (19:29 GMT) | Topic: Security



Internet Explorer's scripting engine was the favorite target of a North Korean cyber-espionage group this year, after the hackers deployed two zero-days, but also crafted new exploits for two other older vulnerabilities.

The group's name is DarkHotel, a cyber-espionage group that McAfee and many other cyber-security firms have already linked to the Pyongyang regime.

The group has been active since 2007, but it was publicly exposed in 2014 when Kaspersky published a now-infamous report detailing a complex hacking operation that involved breaching the internal WiFi networks of hundreds of hotels in order to infect high-profile guests with malware.

Despite being ousted in public reports, DarkHotel didn't stop its attacks, continuing to target victims --and most recently political figures in 2016 and 2017-- with the same tactic.

But they also ran other operations. In one of them, the group -- which in cyber-security circles goes by many different names such as APT-C-06, Dubnium, Fallout Team, Karba, Luder, Nemim, SIG25, and Tapaoux-- also hid malware inside a copy of North Korea's antivirus sent to foreign researchers for study.

DARKHOTEL HACKERS HAD A FIXATION WITH INTERNET EXPLORER

But in 2018, the group has been especially active and has been seen numerous times targeting the same technology --Internet Explorer's VBScript scripting engine.

This year, researchers say DarkHotel hackers found and exploited a first IE zero-day (CVE-2018-8174) in April, and then a second (CVE-2018-8373) in August. Microsoft patched both, in May and September, respectively.

But according to a new report published today, researchers at Qihoo 360 Core say the group has also created new exploits for two older IE scripting engine vulnerabilities --namely CVE-2017-11869 and CVE-2016-0189.

"After analysis, we found that the obfuscation and exploitation of these four [exploits] are highly consistent," said Qihoo 360 Core researchers. "We suspect that they are from the same hacker (or hacking group)."

Zero-days are hard to discover and even harder to weaponize in usable exploits. Creating new exploits for old bugs isn't a walk in the part, either.

We may never know why DarkHotel is expending so many resources into targeting Internet Explorer, but the trend is quite visible for all APT researchers.

IE'S VBSCRIPT ENGINE LIVING OUT ITS LAST DAYS

Internet Explorer's VBScript scripting engine isn't your top notch Microsoft technology either. It's an ancient piece of code from the early days of Windows and Internet Explorer that has always been plagued by quite a large number of vulnerabilities.

Microsoft became well aware of this component's security flaws many years ago. That's why, in July 2017, Microsoft announced that it was disabling the automatic execution of VBScript code in the latest IE version that was included with the Windows 10 Fall Creators Update, released in the fall of last year.

That change meant that hackers couldn't use VBScript code to attack users via Internet Explorer in Windows 10. Microsoft also promised patches to disable VBScript code execution in IE versions on older Windows releases.

That change stopped many cybercrime operations, but DarkHotel seems to have adapted to Microsoft's recent VBScript deprecation announcement.

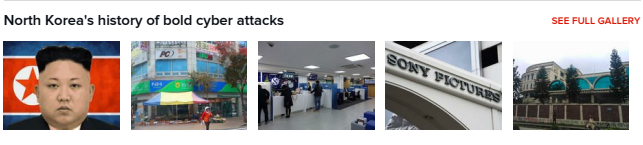
According to reports, DarkHotel apparently opted to use VBScript exploits embedded inside Office documents and did not target Internet Explorer users via the browser directly.

Instead, DarkHotel sent Word documents to victims, documents in which they loaded a malicious web page via embeddable IE frames. DarkHotel hackers chose wisely because, for these instances, VBScript code execution was still permitted.

Based on the current evidence, it appears that in 2018, the group has gone all-in on VBScript exploits before they become totally useless

As Microsoft continues to disable VBScript execution for more and more users, we might have witnessed a cyber-espionage group emptying its VBScript arsenal in a desperate attempt to weaponize hacking tools before they become worthless in the coming years.

North Korea's history of bold cyber attacks SEE FULL GALLERY



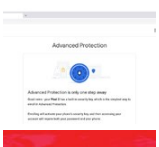
1 - 5 of 12 NEXT ›

RELATED SECURITY COVERAGE:

- Adobe ColdFusion servers under attack from APT group
- Cambodia's ISPs hit by some of the biggest DDoS attacks in the country's history
- US Cyber Command starts uploading foreign APT malware to VirusTotal
- Cisco updates ASR 9000 edge routing platform to carry users to 5G TechRepublic
- Microsoft working on porting Sysinternals to Linux
- Hackers breach StatCounter to hijack Bitcoin transactions on Gate.io exchange
- WPA3 Wi-Fi is here, and it's harder to hack CNET
- Ahead of US midterms, Facebook removes 30 accounts and 85 Instagram profiles

RELATED TOPICS: SECURITY TV | DATA MANAGEMENT | CXO | DATA CENTERS

MORE FROM CATALIN CIMPANU


Security
Google APP users won't be allowed to install apps from outside the Play Store

Security
Two Trend Micro zero-days exploited in the wild by hackers

Security
WordPress and Apache Struts account for 55% of all weaponized vulnerabilities

Tech Industry
Internet's largest social networks issue joint statement on COVID-19 misinformation

NEWSLETTERS

ZDNet Security
Your weekly update on security around the globe, featuring research, threats, and more.
Your email address SUBSCRIBE
SEE ALL

MORE RESOURCES

IT security and privacy: Concerns, initiatives, and predictions (TechRepublic Premium)
Research from TechRepublic Premium
READ NOW

IT Security: Concerns, budgets, trends and plans (TechRepublic Premium)
Research from TechRepublic Premium
READ NOW

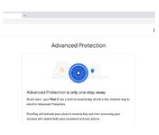
Secrets of an ISA professional
eBooks from TechRepublic Premium
READ NOW

SECURITY

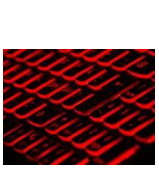
Microsoft shares nightmare tale: 6 sets of hackers on a customer's network
Microsoft orchestrates coordinated takedown of Necurs botnet
This ransomware campaign has just returned with a new trick
Scam, spam and phishing texts: How to spot SMS fraud and stay safe
Cybersecurity: Do these ten things to keep your networks secure from hackers
How to protect yourself from mobile malware attacks (ZDNet YouTube)
Best home security of 2020: Professional monitoring and DIY (CNET)
How to set up secure credential storage for Docker (TechRepublic)

RELATED STORIES 1 of 3


Skimming code battle on NutriBullet website may have risked customer credit card data
The cat-and-mouse game between skimmer installation and removal carried on for weeks.

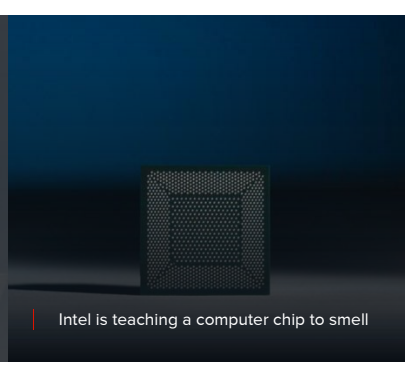


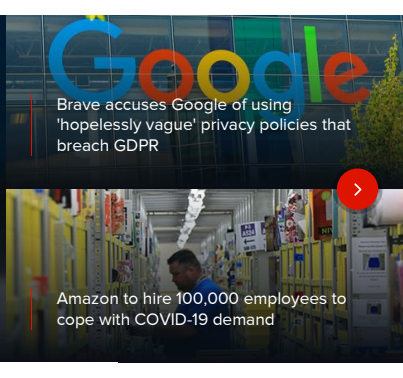
Google APP users won't be allowed to install apps from outside the Play Store
Some exceptions exist, but Google users enrolled in the Advanced Protection Program won't be able to install Android apps from third-party apps stores anymore. ...


VMware patches privilege escalation vulnerability in Fusion, Horizon
Exploits to root systems with Fusion, VMRC or Horizon Client installations were possible.

By Catalin Cimpanu for Zero Day | November 12, 2018 -- 19:29 GMT (19:29 GMT) | Topic: Security

SHOW COMMENTS





JUST IN

Skimming code battle on NutriBullet website may have risked customer credit card data
16 minutes ago

Geo-spatial computing in transportation
26 minutes ago

Google APP users won't be allowed to install apps from outside the Play Store
26 minutes ago

Facebook updates Map With AI service, adds Microsoft Buildings support
26 minutes ago

Slack unveils revamped user interface, with more customization and easier access to apps
26 minutes ago

Microsoft's Windows Terminal now has mouse support for Windows Subsystem for Linux
52 minutes ago

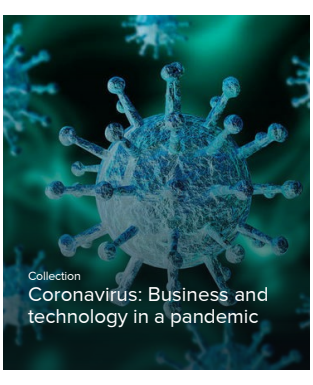
Facebook's new project: To fix time itself
1 hour ago

Work in tech? This is how big a deal the industry has now become
1 hour ago

TODAY ON ZDNET

NEWSLETTERS

ZDNet Announce UK
ZDNet's Announcements newsletter offers a mix of stories, special offers and members-only benefits.
Your email address SUBSCRIBE
SEE ALL




VMware patches privilege escalation vulnerability in Fusion, Horizon
Exploits to root systems with Fusion, VMRC or Horizon Client installations were possible.
2 hours ago by Charlie Osborne in Security

How destructive ransomware attacks could represent the future of cyberwarfare
Nation-state hacking campaigns could masquerade as common criminals conducting ransomware attacks - but their goal would be pure destruction rather than extorting bitcoin, warns a new report.
2 hours ago by Danny Palmer in Security


Windows 10: This kernel malware is why you need Secured-core PCs, says Microsoft
Microsoft's pitch to Windows admins: buy a Secured-core PC so you don't need to configure extra security settings.
2 hours ago by Liam Tung in Security


Coronavirus: Cleaning your phone and keyboard? Here are seven more things you should be disinfecting
Have you adopted a regular cleaning regime for your smartphone and keyboard? Yesterday, completely by accident, I discovered more other things that I should be wiping on a regular basis.
2 hours ago by Adrian Kingsley-Hughes in Hardware


One of the Czech Republic's biggest COVID-19 testing labs hit by cyberattack
The Brno University Hospital in the city of Brno, Czech Republic, has been hit by a misterious cyberattack.
2 hours ago by ZDNet Editors in Security

Trump touts telemedicine: What is it and what do you need to know?
The new face of healthcare for an entire subset of the population will soon be pixelated. We just crash-landed into a massive experiment in treatment from afar.
2 hours ago by Greg Nichols in Digital Health and Wellness

Coronavirus and its impact on the enterprise
COVID-19 has spread to multiple countries, including the United States, causing some businesses and schools to close, disrupting supply chains, and forcing some employees to work remotely from their...
from TechRepublic Premium

Was your Facebook post on the coronavirus deleted? This is why
Anti-spam issues prompted accusations of censorship.
3 hours ago by Charlie Osborne in Security

Geo-spatial computing in transportation

One of the Czech Republic's biggest COVID-19 testing labs hit by cyberattack

Cybersecurity tips for employees who are working from home

Seeking diversity in Australia's intelligence and cybersecurity workforce

ACS will reassess plans to change legal structure

Sharp hit expected for wearables market as COVID-19 impacts China's supply chain

Wyndham Hotels & Resorts tackled technical debt, cloud, hybrid cloud in a hurry [Cloud TV]
HSBC charts out its move to the cloud [Cloud TV]
How Brinker International thinks through cloud, data, Apple iPads [Cloud TV]
Why security is the top barrier in enterprise cloud adoption [Hybrid Cloud TV]
How New Belgium Brewing evaluated managed vs. private cloud [Hybrid Cloud TV]
With Red Hat, IBM to become the leading hybrid cloud provider

Trump touts telemedicine: What is it and what do you need to know?
The new face of healthcare for an entire subset of the population will soon be pixelated. We just crash-landed into a massive experiment in treatment from afar.
2 hours ago by Greg Nichols in Digital Health and Wellness

Coronavirus and its impact on the enterprise
COVID-19 has spread to multiple countries, including the United States, causing some businesses and schools to close, disrupting supply chains, and forcing some employees to work remotely from their...
from TechRepublic Premium

Was your Facebook post on the coronavirus deleted? This is why
Anti-spam issues prompted accusations of censorship.
3 hours ago by Charlie Osborne in Security

Speech Police, book review: How to regain a democratic paradise lost
In Speech Police, David Kaye, lawyer and UN special rapporteur on free opinion and expression, looks for a balance between the human right of free speech and the legitimate need to curb disinformation and abuse.
3 hours ago by Wendy M Grossman in Tech Industry

Cybersecurity tips for employees who are working from home
Switching to remote working because of the coronavirus can create cybersecurity problems for employers and employees. Here are some things to watch.
3 hours ago by ZDNet Editors in Security

Coronavirus: With demand up from so many working from home, will your internet connection survive?
Working from home, school closures, social distancing, and self-isolation have all unprecedented demand on data networks that provide connectivity, video streaming and collaboration. Will your internet connection survive?
4 hours ago by Adrian Kingsley-Hughes in Networking

LOAD MORE

MORE RESOURCES

Secure Browser Usage Policy
Tools & Templates from TechRepublic Premium
READ NOW

GDPR resource kit: Tools to become compliant
Tools & Templates from TechRepublic Premium
READ NOW

Risk Management: Enabling the Business
eBooks from TechRepublic Premium
READ NOW

New Employee Checklist and Default Access Policy
Tools & Templates from TechRepublic Premium
READ NOW