



624TH OPERATIONS CENTER
INTELLIGENCE SURVEILLANCE & RECONNAISSANCE DIVISION



Cyber Threat Bulletin

6 October 2016 (Issue 217)

Prepared by 119 CACS/ISRD / Edited by 624 OC/ISRD (AFCYBER)

The Cyber Threat Bulletin is designed to keep Air Force members knowledgeable of user & network threats. It is located on the AF Portal. It is against our policy to send out this bulletin or request personal data via email. Sources are provided for reference outside official channels.

Breach of Information

According to a Congressional investigation regarding the two attacks set against the Office of Personnel Management's (OPM) network, nation-state threat actors worked in tandem to steal personal information of more than 22 million Americans. The House committee concluded the data breaches reported by OPM in 2014 and 2015 "were likely connected and possibly coordinated." The committee also stated the attack occurred from overseas but did not release the specific location of the attackers. The attackers are believed to have worked on behalf of the Chinese government. The report states the breach is likely the work of Axiom and Deep Panda. Both are known by security experts as Chinese nation-state threat groups who conduct cyber espionage. Both groups used similar malware, attack infrastructure, and MOs in their attacks on OPM.

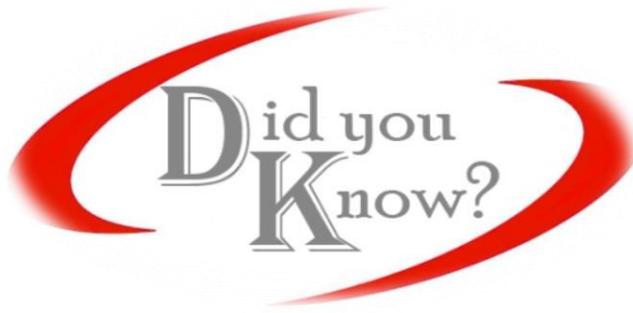


The House committee report criticized OPM for not publicly disclosing the 2014 breach and later declared the 2014 and 2015 attacks were unrelated. However, the attack in 2014 allowed the attackers to establish a presence on the network. The documents taken allowed them to take advantage of OPM and to gain further access into their systems. The House committee assess OPM could have prevented further damage if they would have properly secured its data after the first attack. "All told, some 21.5 million individuals had their social security numbers, residency and employment history, family, health, and financial history exposed in the massive data breach of OPM's background check investigation database. Of the 19.7 million individuals who had applied for the background checks, 1.1 million had their fingerprint scans exposed as well. The remaining

1.8 million people affected by the breach were spouses or other members of the applicants' household."

The House committee also stated the legacy systems at OPM were unable to support encryption and OPM in fiscal years 2013, 2014, and 2015 spent \$7 million per year on cybersecurity, the lowest among agencies. OPM also had "one of the weakest authentication profiles in the government." The report concluded OPM should implement a "zero trust" model for authentication. A zero trust model would require an organization to have multiple levels of authentication and authorization to access data for users inside or outside the agency.

(Information Week Dark Reading: OPM Breach: Two Waves of Attacks Likely Connected, Congressional Probe Concludes; 07 September 2016)



2.5 million Impacted by malware in Google Play

Two newly discovered malicious Android applications in the Google market place may have infected millions of users before they were discovered. The first, CallJam, had between 100,000 and 500,000 installs since it was first uploaded in May 2016. CallJam is hidden inside a game called Gems Chest for Clash Royale and includes a premium dialer to generate fraudulent phone calls. The malware redirects victims to malicious websites with fraudulent advertisements. The Trojan will gain administrative privileges reaching back to a command and control server to initiate premium phone calls and a desired length of the call. This is designed to generate large revenues for the attackers. The app requires acceptance of permissions and will ask the users to rate the app to initiate the malware. The best way Android users can protect against CallJam is to read the reviews and permissions the application is requiring to access the device. Be wary of applications asking permissions to gain accesses to the device seeming suspicious.

The second is the DressCode malware. Approximately 40 apps containing the malicious code were infected in Google Play store and 400 other apps from third-party app stores. Between 500,000 and 2 million users downloaded these infected apps. DressCode creates a botnet of infected devices using ad clicks and false traffic. Check Point mobile security researchers stated Google has removed some of the malicious apps

UNCLASSIFIED//FOR OFFICIAL USE ONLY

from Google play with the oldest apps loaded in April 2016. The DressCode malware is similar to Viking Horde malware, discovered in May 2016. Researchers stated the created botnet could be used to infiltrate internal networks. The malware routes communications on the device to the attacker. This would allow the attacker to access any internal network of the device. Below is a list of the infected apps from the Google Play store.

- com.dark.kazy.goddess.lp
- com.whispering.kazy.spirits.pih
- com.shelter.kazy.ghost.jkv
- com.forsaken.kazy.game.house
- com.dress.up.Musa.Winx.Stella.Tecna.Bloom.Floria
- com.dress.up.princess.Apple.White.Raven.Queen.Ashlynn.Ella.Ever.After.High
- com.monster.high.Dracubecca.freaky.Fusion.draculaura
- com.dress.up.Cerise.Hood.Raven.Queen.Apple.White.Ever.After.Monster.High
- com.ever.after.high.Swan.Duchess.barbie.game
- com.cute.dressup.anime.waitress
- com.rapunzel.naughty.or.nice
- guide.slither.skins
- clash.royale.guide
- guide.lenses.snapchat
- com.minecraft.skins.superhero
- com.catalogstalkerskinforminecraft_.ncyc
- com.applike.robotsskinsforminecraft
- com.temalebedew.modgtavformcpe
- com.manasoft.skinsforminecraftuniquie
- com.romanseverny.militaryskinsforminecraft
- com.temalebedew.animalskinsforminecraft
- com.temalebedew.skinsoncartoonsforminecraft
- com.str.carmodsforminecraft
- com.hairstyles.stepbystep.yyhb
- com.str.mapsfnafforminecraft
- com.weave.braids.steps.txkw
- mech.mod.mcpe
- com.applike.animeskinsforminecraftjcxw
- com.str.furnituremodforminecraft
- com.vladgamerapp.skin.editor.for_.minecraft
- ru.sgejko.horror.mv
- com.vladgamerapp.skins.for_.minecraft.girls
- com.zaharzorkin.cleomodsfortgasailht
- com.temalebedew.ponyskins
- com.my.first.date.stories
- com.gta.mod.minecraft.raccoon
- com.applike.hotskinsforminecraft
- com.applike.serversforminecraftpe
- com.zaharzorkin.pistonsmod
- wiki.clash.guide
- mobile.strike.guide
- prank.calling.app
- sonic.dash.guide

(Security Week: 2.5 Million Possibly Impacted by New Malware in Google Play: 09 September 2016)

For any security related questions, issues, or concerns, contact your Unit Information Assurance Officer, Wing IA and/or the Information Protection Office.

Do you have a question, comment, or concern? Have a topic you would like to see in a future bulletin? Feel free to call us at DSN: 969-0139, or e-mail us at 624oc.isrd@us.af.mil. The use or omission of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

To receive automatic notifications of each new Cyber Threat Bulletin loaded to the AF Portal, select the "Set an Alert" button at the top of the Cyber Threat Bulletins Archive page.

UNCLASSIFIED//FOR OFFICIAL USE ONLY