Pawn Storm Targets German Christian Democratic Union

- Posted on:May 11, 2016 at 8:21 am
- Posted in:Targeted Attacks
- Author: Feike Hacquebord (Senior Threat Researcher)

0

15 51

April last year, Pawn Storm reportedly compromised computers of the German Bundestag using data-stealing malware. This was the first documented political attack of Pawn Storm against Germany. One year later, this espionage actor group takes a swing once again.

In April 2016, we discovered that Pawn Storm started a new attack against the German Christian Democratic Union (CDU), the political party of the Chancellor of Germany, Angela Merkel.

The attack consisted of seemingly coordinated credential phishing attacks against the CDU and high profile users of two German freemail providers. A fake corporate webmail server of CDU was set up in Latvia for advanced credential phishing. Around the same time, three domains were created for credential phishing targeting high-profile individual users of two German free webmail providers. The main fake webmail server of CDU was set up in Latvia, but the free webmail credential phishing sites are on servers of the Virtual Private Server provider in the Netherlands we have discussed previously.

Pawn Storm attackers often conduct sophisticated, simultaneous attacks against targets' corporate and personal email accounts. The attackers build a fake version of the corporate webmail server of the targeted organization and at the same attack key members of the organization on their private free webmail accounts. Credential phishing is an important espionage tool: we have witnessed Pawn Storm downloading complete online e-mail boxes and securing future access by e.g. setting up a forwarding e-mail addresses secretly.

It is a recurring theme in recent Pawn Storm attacks; organizations get hit from different angles simultaneously. We have seen that happening time and time again against various governments, armed forces, defense companies and media.

Prior to this attack, we reported on Pawn Storm attacking the Turkish government from various angles last March 2016. These attacks further confirm our theories as to the identities of the attackers. Pawn Storm clearly targets groups that could be perceived as a risk to Russian politics and interests.

Even though Pawn Storm is one of the oldest active espionage threat actors (we can trace activity back to 2004), it still remains very active, attacking many targets worldwide simultaneously at a high rate both with credential phishing and malware. Monitoring it's recent activity, we have counted over a dozen live

X-Agent Command and Control servers. X-Agent is second stage malware of Pawn Storm that will only be used against high-value targets that are of particular interest. This is another strong indication how active Pawn Storm is.

The following are the domains mentioned in the article:

- account-web[.]de
- account-gmx[.]de
- account-gmx[.]net

Related Posts:

- **Pawn Storm Targets MH17 Investigation Team**
- **Pawn Storm’s Domestic Spying Campaign Revealed; Ukraine and US Top Global Targets**
- **Pawn Storm Campaign Adds Turkey To Its List of Targets**
- **New Adobe Flash Zero-Day Used in Pawn Storm Campaign Targeting Foreign Affairs Ministries**

Tags: CDUGerman Christian Democratic UnionGermanyPawn Stormtargeted attacks

0 Comments TrendLabs 1 Login

Recommend Share Sort by Best

Start the discussion…

Be the first to comment.

Subscribe Add Disqus to your site Add Disqus Add Privacy

Featured Stories

- The Panamanian Shell Game: Cybercriminals With Offshore Bank Accounts?
- Dark Motives Online: An Analysis of Overlapping Technologies Used by Cybercriminals and Terrorist Organizations
- Crypto-ransomware Gains Footing in Corporate Grounds, Gets Nastier for End Users
- SpyEye Creator Sentenced to 9 Years in Federal Prison
- Indian Military Personnel Targeted by “Operation C-Major” Information Theft Campaign

Recent Posts

- LinkedIn Breach: More Questions than Answers
- Kernel Waiter Exploit from the Hacking Team Leak Still Being Used
- Flashlight App Spews Malicious Ads
- New Flash Vulnerability CVE-2016-4117 Shares Similarities With Older Pawn Storm Exploit
- Chinese-language Ransomware Makes An Appearance

Cybercrime Across the Globe: What Makes Each Market Unique?

- This interactive map shows how diverse the cybercriminal underground economy is, with different markets that are as unique as the country or region that it caters to.
  Read more

Business Email Compromise

- A sophisticated scam has been targeting businesses that work with foreign partners, costing US victims $750M since 2013.
  How do BEC scams work?

Popular Posts

Data Protection Mishap Leaves 55M Philippine Voters at Risk
New Crypto-Ransomware JIGSAW Plays Nasty Games
Locky Ransomware Spreads via Flash and Windows Kernel Exploits
Hacking Team Flash Zero-Day Integrated Into Exploit Kits
Cybercriminals Improve Android Malware Stealth Routines with OBAD

Latest Tweets

- Read how the #BlackEnergy cyber attack could point to a dark future: bit.ly/200S4f3
  about 56 mins ago
- New post: LinkedIn Breach: More Questions than Answers bit.ly/1XDXApa @TrendMicro
  about 5 hours ago
- Meet #BlackEnergy, the malware that can cripple a nation’s infrastructure bit.ly/200S4f3 #cybersecurity
  about 5 hours ago

Stay Updated

Email Subscription

Your email here

Subscribe