Does a BEAR Leak in the Woods?
The DNC Breach, Russian APTs, and the 2016 US Election

Toni Gidwani
Director of Research Operations
@t_gidwani
Today’s Agenda

- The DNC Breach
- Guccifer 2.0
- The DCCC Breach
- DCLeaks and Spearphishing
- Conclusions
From Russia, With Love
The Basics of the Breaches and Bears
The DNC Breach

14 June

- Washington Post article reports breach, cites CrowdStrike attribution to Russian Advanced Persistent Threat (APT) groups
  - FANCY BEAR
  - COZY BEAR

Separate breaches

- No evidence the two groups knew the other was there
**Cozy Bear**

**Background**

- AKA CozyDuke, APT 29
- Uses sophisticated RATs with extensive anti-analysis techniques
- Broadly targeted spearphish campaigns with links to a malicious dropper
- Linked to intrusions into unclassified White House, State Department, and U.S. Joint Chiefs of Staff networks

**DNC Breach**

- Breached DNC in Summer 2015
- SeaDaddy implant developed in Python and a Powershell backdoor stored only in WMI database
- Allowed the adversary to launch malicious code automatically at will, executing in memory
- Powershell version of MimiKatz used to acquire credentials for lateral movement

© 2017 ThreatConnect, Inc. All Rights Reserved.
Background

- AKA Sofacy, APT 28
- Assessed GRU, Russia’s primary military intelligence service
- Implants include Sofacy, X-Agent, X-Tunnel, WinIDS droppers
- Steals victim credentials by spoofing their web-based email services
- Linked to intrusions into the German Bundestag and France’s TV5 Monde

DNC Breach

- Breached DNC in April 2016
- X-Agent malware with capabilities to do remote command execution, file transmission and keylogging
- X-Tunnel network tunneling tool
- Anti-forensic measures such as periodic event log clearing and resetting timestamps of files
Meanwhile,

At ThreatConnect...
- Started looking for other BEAR infrastructure
- Shared out the CrowdStrike analysis
### Passive DNS

<table>
<thead>
<tr>
<th>Host</th>
<th>First Seen Resolution</th>
<th>Last Seen Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>newtoro.com</td>
<td>Thu Dec 31 17:09:18 UTC 2015</td>
<td>Fri Jan 22 06:46:52 UTC 2016</td>
</tr>
<tr>
<td>uz5gz6b9t16s6i066x707dj9h2s62w2huqvb7506byg777h909.ns.blii</td>
<td>Tue Sep 01 19:20:47 UTC 2015</td>
<td>Sat Dec 12 08:58:51 UTC 2015</td>
</tr>
<tr>
<td>t.section8dot.com</td>
<td>Thu Aug 06 23:04:45 UTC 2015</td>
<td>Sat Oct 31 00:50:41 UTC 2015</td>
</tr>
</tbody>
</table>
Pivoting Through the Data
Legitimate MIS Department domain:
- Lists DNC as a client
- Spoofed domains a common tactic
Guccifer 2.0

- Emerged on 15 June, just after DNC breach is reported, with a Wordpress blog
- Twitter handle created on 20 June
- Borrowed Guccifer name from jailed Romanian hacker Marcel Lazăr Lehel

His Claims:
- “Hacked” the DNC in Summer 2015
- Romanian, with no affiliation to Russia
- Motivated to create a world “free from Illuminati”

His Actions:
- Posts purloined docs on his blog
-Leaks docs via journalists and WikiLeaks
The More He Talks About the Breach, The Less Plausible It Sounds

Claim: Found 0-day in NGP VAN, a niche SaaS platform
  • Fuzzing, IDA Pro, WinDbg

Problem: Targeted platform is a multi-tenant cloud solution
  • No local binary to fuzz, disassemble, or debug
  • Word choice in responding suggests lack of technical expertise

Claim: Compromised the DNC last summer
  • Exploited bug that gave Sanders campaign unauthorized access to voter information

Problem: Bug did not exist until December 2015
  • Only Chuck Norris can exploit a vulnerability for software that has not yet been written
Hacktivist or Faketivist

VS
Getting to Know Journalists

Leaked Documents Directly To:
- The Smoking Gun
- The Hill
- Vocative

Reporters say Guccifer 2.0 is pushing hard for them to publish, but docs are not really newsworthy

13 July: Guccifer 2.0 tells The Hill “The press [is] gradually forget[ing] about me, [W]ikileaks is playing for time and [I] have some more docs.”

Reporters from these publications share the email headers with ThreatConnect for analysis
Tracing Guccifer 2.0 Infrastructure Back to a Russian VPN

The French Connection

- French Twitter account
- French AOL account - guccifer20@aol[.]fr
- Originating French IP - 95.130.54[.]34

What’s on That IP?

- OpenSSH and Point-to-Point Tunnelling
- SSH fingerprint shared with six other IPs

Not a Tor Node, but Russia’s Elite VPN Service

- vpn-service[.]us
- sec.service@mail[.]ru original registrant
- All IPs offered share the same SSH fingerprint
- Guccifer 2.0’s IP not publicly available
22 July: WikiLeaks dump

WikiLeaks releases thousands of documents about Clinton and internal deliberations

By Tom Hamburger and Karen Tumulty

DNC Chair Debbie Wasserman Schultz to Resign Amid Email Hack

Ms. Wasserman Schultz, who will step down at the end of this week’s convention, plans to address the delegates

By Laura Meckler

Updated July 24, 2016 4:41 p.m. ET

PHILADELPHIA—The chairwoman of the Democratic National Committee resigned Sunday after a trove of emails were disclosed showing DNC officials had worked to undermine the underdog presidential campaign of Vermont Sen. Bernie Sanders.
The DCCC Breach

- **29 July:** Reuters article reports breach, cites FBI investigation
- **Indicator characteristics previously linked to FANCY BEAR**
- **12 Aug:** Guccifer 2.0 publishes documents obtained via the breach
Spoofed donation website `actblues[.]com`

- `fisterboks@mail[.]com` previously registered three other domains linked to FANCY BEAR
- Registered on 14 June - timing consistent with DNC breach announcement
- Same name servers used by `frank_merdeux@europe[.]com`
Guccifer 2.0 Shows Us DCLeaks

27 June: In emails with *The Smoking Gun*, Guccifer 2.0 directs reporter to DCLeaks

- Content is password protected
- Asks reporter not to mention him in connection with DCLeaks

*TSG* sees Rinehart profile on the site, contacts him, gets a copy of spearphish for ThreatConnect

Other notable profiles: General (ret.) Phillip Breedlove, George Soros, Republicans
Background

- Established in April 2016
- Claims to be a “new level project” initiated by “the American hacktivists”
- Registered by feehan@europe[..]com
- Name server also hosted domains associated with FANCY BEAR
FANCY BEAR Spearphishing

March 2016 spearphishing campaign targeting Clinton campaign staff

- Spearphish claims suspicious login activity and requests user change password
- Used Bitly to shorten malicious links
- Base64-encoded string containing the victim's full email address is passed with this URL, prepopulating a fake Google login page displayed to the victim

Published by SecureWorks Counter Threat Unit on 16 June
• 22 March: Spearphish sent to DNC regional field director

• Sent from hi.mymail@yandex[.]com

• Looked like a Google security notification

• Contained a link to a bit.ly shortened URL
  • Clicked once on 20 March 2016
  • Faux Google login page: myaccount.google.com-securitysettingpage[.]ml

• Facilitated “Man in the mailbox” attack
State Boards of Elections

Background

• Jul - Aug 2016
• Arizona and Illinois

MAR-AUG 2016: Hosted a spearphishing campaign targeting Turkish and Ukrainian government officials
  • SO WHAT: Victims and tactics consistent with Russian APT targeting; activity atypical for criminals

JAN-MAY 2015: Hosted a Russian criminal forum
  • SO WHAT: Suggests Russia-based link; low attribution value

Circumstantial evidence: 5.149.249.[172 hosted on FortUnix infrastructure. Other FortUnix infrastructure seen in 2015 Ukraine power grid and news media denial of service attacks

WHAT: Open source tools used closely parallel stainpoland's description of how they obtained athlete records from World Anti-Doping Agency

SO WHAT: @anpoland a possible, but unconfirmed, strategic leak outlet. Capabilities leveraged are widely available, non-diagnostic alone for attribution

WHAT: 6 IP addresses hosted on King Servers, a Russian-owned hosting service

SO WHAT: Suggests Russia-based link; low attribution value

© 2017 ThreatConnect, Inc. All Rights Reserved.
The BEAR Essentials

- Fingerprints of known Russian APT threat actors identified
- Multiple venues to breach and leak data
- Victims consistent with known targeting focus
Joint Analysis Report (JAR) on GRIZZLY STEPPE

- Outlines GRIZZLY STEPPE indicators and analysis of GRIZZLY STEPPE activity
- Includes over 870 IP Addresses to enable network defenders to identify activity from these actors
Using ThreatConnect to Get More Context

- Entered indicators in ThreatConnect’s ‘Analyze’ function to see if they were associated with any known adversaries

- **Connected GRIZZLY STEPPE JAR IPs to FANCY BEAR**, and then added more indicators and context
  - Hosting history
  - Registrant information

- Pivoted out from GRIZZLY STEPPE provided intel to identify new IPs, domains, and other registrants associated with FANCY BEAR
The Results

What We Did

- Associated 43 of the first 80 IPs in the GRIZZLY STEPPE JAR with FANCY BEAR
- Used ThreatConnect to generate an additional 122 indicators, including 68 domains, 17 IPs, and 15 email registrants
- Significantly augmented the context for some of the indicators included in the JAR and trace out from those indicators to provide enriched indicators for FANCY BEAR
- Shared our findings with the ThreatConnect Common Community in Incident 20170106A: Fancy Bear Indicators Identified from Research into USG JAR on GRIZZLY STEPPE
Conclusions
The Good, the Bad, and the Ugly

Worst case: Interfere with U.S. ability to hold a credible election in November
  • Precedent: CyberBerkut activity against Ukrainian government during 2014 election

Damage individual politicians by leaking embarrassing data

Undermine faith in government processes and leadership

Amplify these messages through Russian propaganda channels and media for domestic Russian audience

Dumping large amounts of personal data is deemed totally acceptable
The Value of Good Analytic Tradecraft

**Technical**

Infrastructure analysis
- Passive DNS
- WHOIS
- Start of Authority records
- Name Servers

Develops picture of adversary TTPs

**Strategic Context**

The Diamond Model of Intrusion Analysis

Structured Analytic Techniques
- Analysis of Competing Hypotheses

**Info Sharing**

Working with a number of reporters to:
- Broaden the pool of additional indicators
- Identify TTPs
- Provide I&W of new campaigns

Extract max intel value from government provided intel
25 Jan: Stepping to Fancy Bear
- Identifying context from the JAR on GRIZZLY STEPPE

13 Dec: Hacktivists vs Faketivists: Fancy Bears in Disguise
- Reviews FANCY BEAR-Linked Faketivists

18 Oct: Let’s Get Fancy
- How our team conducted analysis regarding FANCY BEAR

28 Sep: Belling the BEAR
- Reviews activity targeting Bellingcat

2 Sep: Can a BEAR Fit Down a Rabbit Hole?
- SBOE Attacks and TUR/UKR Spearphishing

19 Aug: Russian Cyber Operations on Steroids
- Attacks Against WADA

12 Aug: Does a BEAR Leak in the Woods?
- Identifies DCLeaks as another Russian-backed influence outlet

29 Jul: FANCY BEAR has an (IT) Itch They Can’t Scratch
- DCCC breach infrastructure

26 Jul: All Roads Lead to Russia
- Review of French infrastructure associated with Guccifer 2.0’s media communications

- Update to previous Guccifer 2.0 evaluation and projections for the persona’s future use

7 Jul: What’s in a Name Server
- Identifies additional suspicious infrastructure based on name servers

29 Jun: Shiny Object
- Evaluation of hypotheses on Guccifer 2.0’s true identity

17 Jun: Rebooting Watergate
- Additional research into the DNC breach and associated infrastructure
Thank You
THREATCONNECT.COM
@t_gidwani