



Department of Energy

Bonneville Power Administration
P.O. Box 3621
Portland, Oregon 97208-3621

FREEDOM OF INFORMATION ACT PROGRAM

February 24, 2020

In reply refer to: FOIA #BPA-2020-00414-F

Kartikay Mehrotra
Bloomberg News
Pier 3 Suite 201
San Francisco, CA 94111
Fax: 415-617-7620
Phone: 415-617-7173
Email: kmehrotra2@bloomberg.net

Dear Mr. Mehrotra,

Thank you for your interest in the Bonneville Power Administration (BPA). The agency received your request for records made under the Freedom of Information Act, 5 U.S.C. § 552, (FOIA). Your request was received on January 27, 2020 and assigned control number BPA-2020-00414-F. Please use this number in any correspondence with the agency about your request.

Request

“Pursuant to the Freedom of Information Act, 5 U.S.C. Section 552 et seq. ("FOIA"), I request access to and copies of the Bonneville Red Team Report published between October 2014 and April 2015 (“the Records”). This request is ongoing, seeking copies of (or access to) all Records as they are filed with the Department of Energy. I am further requesting that the Records be provided to me on computer files or, if not maintained on computer files, in the same format as they are currently maintained at the Department of Energy.”

Response

The agency located 21 pages of records responsive to your request. BPA is herein releasing all pages with four pages containing minimal redactions applied under 5 U.S.C. § 552(b)(5) (Exemption 5).

Exemptions

The FOIA generally requires the release of all responsive government records upon request. However, the FOIA permits withholding certain limited information that falls under one or more of nine statutory exemptions (5 U.S.C. §§ 552(b)(1-9)).

Exemption 5

Exemption 5 protects “inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency” (5 U.S.C. §

552(b)(5)). In plain language, the exemption protects privileged records. The FOIA's Exemption 5 deliberative process privilege protects records evincing the deliberative or decision-making processes of government agencies. Records protected under this privilege must be both pre-decisional and deliberative. A record is pre-decisional if it is generated before the adoption of an agency policy. A record is deliberative if it reflects the give-and-take of the consultative process, either by assessing the merits of a particular viewpoint, or by articulating the process used by the agency to formulate a decision. BPA has considered and declined a discretionary release of some pre-decisional and deliberative information in the responsive records set because disclosure of the records would harm the interests protected and encouraged by Exemption 5. In this case, BPA asserts Exemption 5 to protect BPA Cyber Security staff viewpoints and recommendations expressed in the report.

Fees

There are no fees associated with the response to your request.

Certification

Your FOIA request BPA-2020-00414-F is now closed with all available agency records provided. Pursuant to 10 C.F.R. § 1004.7(b)(2), I am the individual responsible for the exemption determinations and records release described above.

Appeal

The adequacy of the search may be appealed within 90 calendar days from your receipt of this letter pursuant to 10 C.F.R. § 1004.8. Appeals should be addressed to:

Director, Office of Hearings and Appeals
HG-1, L'Enfant Plaza
U.S. Department of Energy
1000 Independence Avenue, S.W.
Washington, D.C. 20585-1615

The written appeal, including the envelope, must clearly indicate that a FOIA appeal is being made. You may also submit your appeal by e-mail to OHA.filings@hq.doe.gov, including the phrase "Freedom of Information Appeal" in the subject line. (The Office of Hearings and Appeals prefers to receive appeals by email.) The appeal must contain all the elements required by 10 C.F.R. § 1004.8, including a copy of the determination letter. Thereafter, judicial review will be available to you in the Federal District Court either (1) in the district where you reside, (2) where you have your principal place of business, (3) where DOE's records are situated, or (4) in the District of Columbia.

You may contact BPA's FOIA Public Liaison, Jason Taylor, at 503-230-3537, jetaylor@bpa.gov, or the address on this letter header for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road-OGIS
College Park, Maryland 20740-6001
E-mail: ogis@nara.gov
Phone: 202-741-5770
Toll-free: 1-877-684-6448
Fax: 202-741-5769

Thank you again for your interest in the Bonneville Power Administration.

Sincerely,

A handwritten signature in black ink, appearing to read "Candice D. Palen". The signature is fluid and cursive, with the first name being the most prominent.

Candice D. Palen
Freedom of Information/Privacy Act Officer

Official Use Only

May be exempt from public release under the
Freedom of Information Act (5 U.S.C. 552),
Exemption Number 3 - Circumvention of Statute

BPA Review required before public release.

Name: Gary Dodd Org: JB Date: 9/22/2014

Enterprise Penetration Testing
“Red Team” Report Q4 FY2014
BPA Office of Cyber Security

October 2014

Table of Contents

Executive Summary	4
Background	5
Introduction.....	6
Cyber Kill Chain®	6
External Activity on BPA	7
Passive reconnaissance	7
Active reconnaissance.....	8
Weaponization	9
Delivery	9
Exploitation, Installation and C2	9
Internal Activity on BPA User Domain (BUD).....	10
Active reconnaissance.....	10
Exploitation.....	12
.....	12
Installation and C2	12
Action on Objectives.....	13
Exploitation.....	14
Internal Activity on other BPA networks	14
.....	16
Field Information Network (FIN)	16
Active reconnaissance.....	16
Weaponization	17
Delivery and Installation.....	17
Exploitation and Actions on Objectives.....	17
Control Center Network (CCN).....	18
Active reconnaissance.....	18

Actions on Objectives (lateral movement).....	18
Active reconnaissance.....	19
Weaponization	19
End of Exercise	20
Recommendations.....	20
Appendix A: Definitions.....	21

Executive Summary

On April 8th, 2014 the BPA Office of Cyber Security Assessment team successfully launched an Advanced Persistent Threat (APT) campaign that compromised the BPA internal network and installed malicious software that gave complete access to internal BPA networks from the outside. During the compromise, the team was able to exfiltrate large amounts of sensitive BPA data without detection.

BPA's Office of Cyber Security routinely conducts security assessments of BPA systems as part of the security authorization process. These assessments provide an individual viewpoint of IT/OT systems, which is necessary to meet compliance mandates but does not provide a holistic enough picture of the organizational security risk. In order to supplement the assessment efforts and better understand the exploitable vulnerabilities, specifically how to detect and mitigate them, the Cyber Security Assessment team performs 'red team' exercises.

This is the first time we have tested the entire enterprise holistically as opposed to attacking or assessing a single system. As well, this particular exercise had Cyber personnel acting as malicious actors from the Internet with no inside knowledge.

Attackers use a broad spectrum of tools and tactics that includes social media, social engineering and circumventing physical access in order to compromise networks. The Red Team exercises test how well people, process and tools can defend, detect and respond against emulated threat actor techniques, tactics and procedures (TTPs).

The assessment team began reconnaissance activity by performing open-source intelligence (OSINT) gathering activity. This activity discovered BPA Freedom Of Information Act (FOIA) requests relating to BPA systems and employee information, which provided some valuable system and contact information. Job postings, professional networking sites and domain name searches provided additional information on software, technology and networks used by BPA.


The team then used the OSINT information to actively scan the BPA network from outside of BPA, looking for well known vulnerabilities, services and other targets of opportunity. The results pointed to several additional areas for possible exploitation and the assessors moved into active exploitation.

Phishing emails were crafted and sent to 35 BPA users. A malicious Excel file was attached to these emails that, when executed, provided a means to bypass network defenses and ability to remotely access the BPA HQ network from the outside. Using these connections, the Red Team attackers were able to impersonate the individuals who had opened the file, making it appear that any actions performed were by that BPA user.

Once inside BPA's network, the team was able to collect information on all employee user accounts; this allowed them to identify privileged user accounts, computers, and groups. Employing password guessing techniques over a 28 day period, they identified several commonly used password combinations at BPA. The attackers identified, and were able to take control of, over 30 physical security cameras and numerous appliances connected to the network, mostly due to default configurations. From inside the BPA HQ network, the team was able to perform lateral movement within and between other internal BPA networks.

The team was able to access and install malware on 38 workstations that are routinely and almost constantly connect to the FIN (Field Information Network) and the business administrative network. These workstations are referred to as instrument controllers, or instrument controllers dual-purpose. Operating on both the IT network and the FIN is a necessary part of the job function for these devices and the craftsman that use them. They are used to remotely and locally access breakers and relays and can be used to open and close these breakers. The malware allowed the Red Team to successfully exfiltrate sensitive data from these systems without detection.

The introduction of malware on this equipment can run autonomously and not require a network connection. The gateways that allow access into the electric equipment are systems categorized as high using federal information processing standard (FIPS 199). (b) (5)



In addition, the team successfully infiltrated the Control Center DMZ (a sub network that contains and exposes external-facing services to the Internet). The domain is referred to as DGOZ. The simulated attackers were able to remotely connect to this network using BPA HQ network credentials. They then were able to guess administrator credentials through password reuse and pattern matching. The attackers were able to modify webpages of DGOZ internal websites, gain full access to an internal file server and deploy malicious code on internal web pages. Although one of the malicious files was found after nearly 4 weeks, and the exercise was ended, incident response mechanisms were not initiated and the absence of that file would not have stopped the next phase of the attack.

The exercise has proven that an external threat can successfully penetrate internal BPA systems with minimal detection or response. The team has documented the detailed activities performed during the exercise and will make available known mitigation techniques for the vulnerabilities discovered.

High-level recommendations include:

- (b) (5)
- [Redacted]
- [Redacted]

Background

The Federal Information Security Management Act (Title III of the e-government act) assigns the authority and responsibility for periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented to the senior agency information security officer. The BPA cyber security program provides a mechanism to help BPA evaluate, prioritize, and improve its cybersecurity capabilities while improving our maturity level in order to align with the statutory requirement to cost-effectively reduce information security risks to an acceptable level.

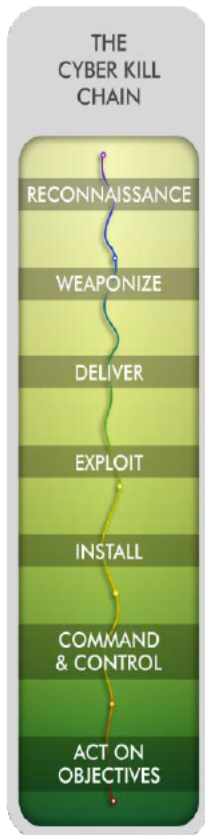
Introduction

In April 2014, the BPA Office of Cyber Security began an Advanced Persistent Threat (APT) exercise. While BPA's Office of Cyber Security conducts regular security assessment of BPA systems, this is the first time the office has tested the entire enterprise holistically as opposed to attacking or assessing a single system. This exercise was designed to evaluate the infrastructure from an outside attacker's perspective to determine how well it protects BPA, its mission, systems and personnel from external threats. The activity also provides a means of evaluating BPA's incident response procedures.

The attack will be described using the Cyber Kill Chain® model developed by Lockheed Martin. The kill chain is a systematic process to target and engage an adversary to create desired effects. BPA Cyber Security has adopted the approach of an intelligence-driven computer network defense in its cyber operations and the Cyber Kill Chain® is an important concept in that approach.

Cyber Kill Chain®

1. **Reconnaissance** - Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies.
2. **Weaponization** - Coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents serve as the weaponized deliverable.
3. **Delivery** - Transmission of the weapon to the targeted environment. The three most prevalent delivery vectors for weaponized payloads by APT actors, as observed by the Lockheed Martin Computer Incident Response Team (LM-CIRT) for the years 2004-2010, are email attachments, websites, and USB removable media.
4. **Exploitation** - After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code.
5. **Installation** - Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.
6. **Command and Control (C2)** - Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. APT malware especially requires manual interaction rather than conduct activity automatically. Once the C2 channel establishes, intruders have "hands on the keyboard" access inside the target environment.
7. **Actions on Objectives** - Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically, this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well. Alternatively, the intruders may only desire access to the initial victim box for use as a hop point to compromise additional systems and move laterally inside the network.



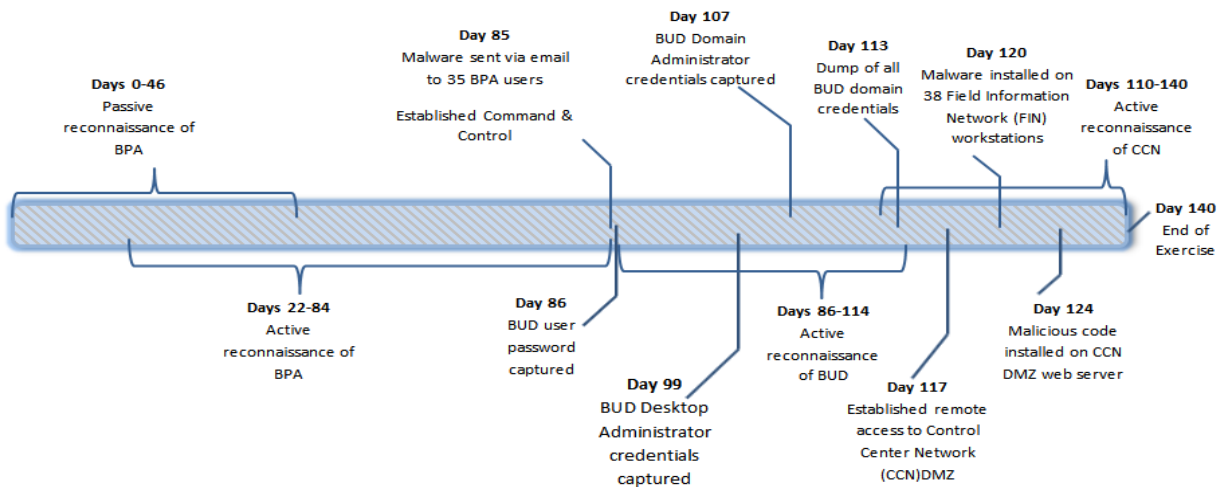
© 2014 Lockheed Martin Corporation

This activity has been documented and designed by the Chief Information Security Officer and approved by the Chief Information Officer (CIO) and VP of Information Technology.

Rules of engagement

1. No damage (example: intentional denial of service or changes to data) shall occur that would impact integrity of BPA's production systems. If a weakness is found that could potentially damage BPA systems, approval from the BPA CISO is required to exploit;
2. No prior knowledge can be leveraged for exploits, only weaknesses found during the exercise could be exploited, attackers are to act as outsiders;
3. Evidence of each discovered weakness and exploit will be maintained along with information about what would have prevented and what would have detected the attacks at each step of the cyber kill chain.

Activity Timeline



External Activity on BPA

Passive reconnaissance

The exercise was initiated from an external network (not owned or used by BPA). Approximately one month was spent gathering information on BPA assets by utilizing this external network and open source intelligence (OSINT) information gathering. Part of the OSINT information gathering phase focused on searching public search engines for Bonneville specific keyphrases (ie. "inurl:bpa.gov -site:www.bpa.gov").



A search used to find PDF files, returned a 2013 FOIA request which listed email accounts, names, and phone numbers for all BPA federal employees. Other searches returned files which identified employees with elevated system privileges. Identification of users with specific privileges, and access, allowed the attackers to target specific users for subsequent attacks.

Next, the assessment team searched the professional networking site “LinkedIn” for specific users identified in prior OSINT tactics. This search provided names and titles of federal and contract employees, as well as some employee’s personal profiles that identified hardware and software currently in use. Additionally, searches of various publicly available databases identified specific servers and network names associated with BPA, giving the attackers a map of the organization’s external facing perimeter.

During this phase, it was determined that the primary sources of information relating to BPA systems are professional networking sites, such as LinkedIn, and FOIA requests.

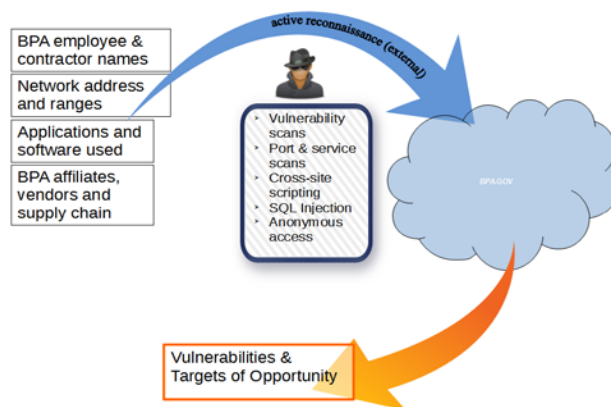
Active reconnaissance

The attackers then leveraged information gathered during passive reconnaissance in an attempt to infiltrate the internal BPA network(s). They began by manually probing the external servers for well known vulnerabilities using a “low and slow” strategy to avoid detection. They were able to identify several servers in the 170.160.x.x range. Next they probed the identified servers using NMAP, on a limited set of ports, to determine which ones were accessible from outside the BPA network. While these probes required several days to complete, they were not noticed by BPA. Only 4 ports were identified as open from the outside (21, 25, 80, and 443).

Concentrating on ports 80 and 443, the attackers tested for 5 common types of web application vulnerabilities: *Cross Site Scripting*, *SQL Injection*, *Remote-File-Includes/Local-File-Includes*, *File Upload* and *Directory Guessing*. All the testing was performed behind anonymous proxies. Directory guessing was performed using an automated tool called “DirBuster”.

What follows is a list of findings from the active reconnaissance activities:

- External cross-site scripting vulnerabilities were found but not utilized in this attack.
- Potential SQL-injections were found but the attackers determined exploiting them would be too “noisy” and easily detected, further they did not appear to be useful for compromising the housing server(s).
- A remote file inclusion vulnerability was found but not weaponized.
- The scans by DirBuster were inadvertently detected by DoE’s Cooperative Protection Plan (CPP) sensors when a User-Agent string was detected by canned IDS signatures.
 - It took 10 days for BPA’s Cyber Security to be notified of this detection, indicating a weakness in BPA’s Incident Response process.
- An FTP server allowing anonymous file uploading and downloading was discovered but was not utilized in this attack
- Several SMTP mail servers were identified. Three of the mail servers allowed outside users to email internal users while faking the source mailing address as an internal user.

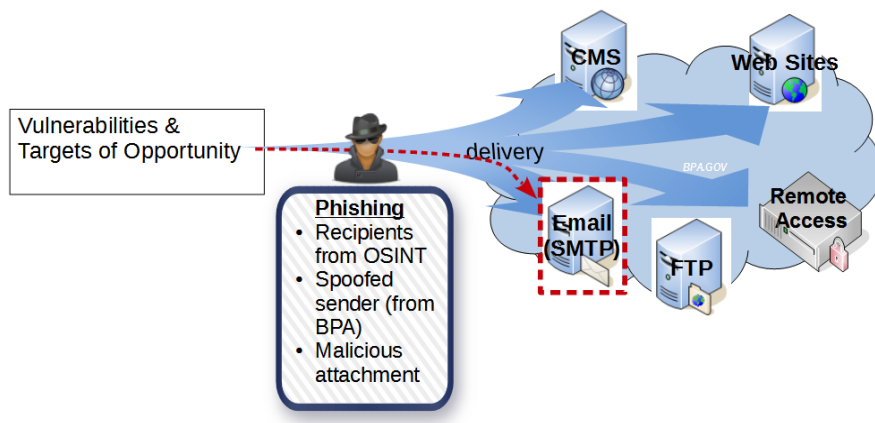


- On one of the mail servers, Sophos blocks the faked sending address but gives a warning message with a Sophos link to where the spoofed address can be white-listed. This allowed the attackers to bypass the protection mechanism and successfully send malicious email into the organization.

Weaponization

The attackers then moved into active exploitation. Based on the results of the reconnaissance phase, the Team decided social engineering (through a **Phishing Attack**) would likely provide the best results. Initially they attempted to use a Microsoft Word document containing a malicious macro as the payload. The Team tested the use of an infected MS Excel file on a machine built with Microsoft Forefront. The Microsoft Anti-malware software did not detect the malware.

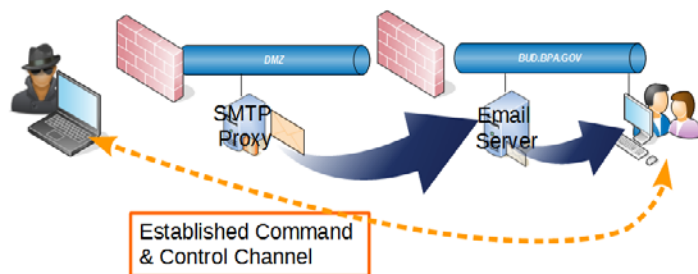
Delivery



The attackers created an email concerning a news article that appeared to originate from www.bpa.gov. Using the email addresses gathered during the OSINT (phase 1), an email was sent to 35 individuals, from a public network, containing the infected Excel document. Four of the recipients opened the Excel file, launching the embedded macro.

Exploitation, Installation and C2

The Excel macro launched a reverse connection back to the Team's *Command-and-Control*(C2) server on the internet (not the same IP address used to launch the attack). Using these connections, the Team was able to impersonate the account of the individuals who had opened the Excel file. Should anomalies have been detected, it would appear the attacked employees were responsible since any action taken used their valid userid. The virtualized nature of MyPC made an attack very difficult to maintain.



Since the user's environment is recreated every time the user logs on, the Team had to determine an easy way to maintain persistence with the code giving them access across logins. The login.bat file was chosen as an executable that could be appended by the malware. Due to an error in the macro's delivered malware, an error in the login.bat file was detected and the Team lost all access. The Team identified the situation in real time, made modifications to end further detection, and extended their functionality within the network. If the IT Operations people had realized what was happening it could have stopped the attack. However control was re-established. All subsequent C2 activity went unnoticed on the BUD network. No report of a possible phishing attack was reported by any of the recipients.

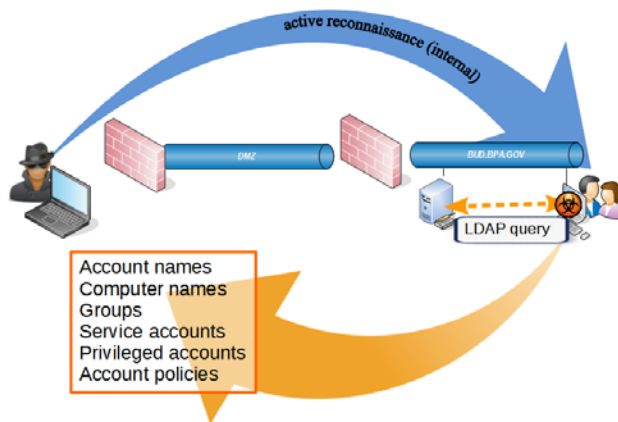
Internal Activity on BPA User Domain (BUD)

Active reconnaissance

File-share and internal SharePoint scavenging

Once inside BPA's network, the Teams leveraged tools available to any authenticated user. Using these tools they were able to collect information on all employee user accounts; this allowed them to identify privileged user accounts, computers, and groups.

- Many users have a second account starting with "epu" for *Elevated Privilege User*. A few of the accounts also had information in the info field.
- Many of the computer accounts contained the name of the "owner" thus allowing the attackers to cross reference the output listing from Active Directory with the Freedom of Information Act (FOIA) listing of government employees.
- Non-IT developers were also assigned "epu" accounts for developing programs using the "R" language for statistical development.
- Elevated privileges are also required for any user of the Aurora application. This is due to the application generating databases as output.
- Many of the Active Directory groups contained the word "Admin" in the group name.



Automated Password Guessing

Using the command "c:\> net accounts", the Team were able to discover the password policy for BPA. Using this information they discovered the maximum number of logon attempts available before the account locked. Additionally, if an account was inadvertently locked they knew how long before it would unlock automatically.

Next, the team attempted four passwords per account every 30-60 minutes for every account. In addition to identifying the accounts the attackers could exploit, they were also able to identify commonly used password combinations. This password guessing scan ran over the entire business administrative network for over a month and was only detected by one group, Critical Business Systems (JC). The account activity was discovered after JC began leveraging the new instance of Splunk. Splunk is software implemented and used by the Cyber Security Operations and Analysis Center (CSOAC). The team terminated the password guessing activity at that point.

Internal Port Scans

The Team chose to execute “low-and-slow” NMAP port scans of ports 80 and 443 on the entire 10.0.0.0/8 subnet resulting in approximately 3248 responses. The rationale for the “*low-and-slow*” scan was to prevent any potential Host-based Intrusion Prevention System (HIPS) detecting the scans.

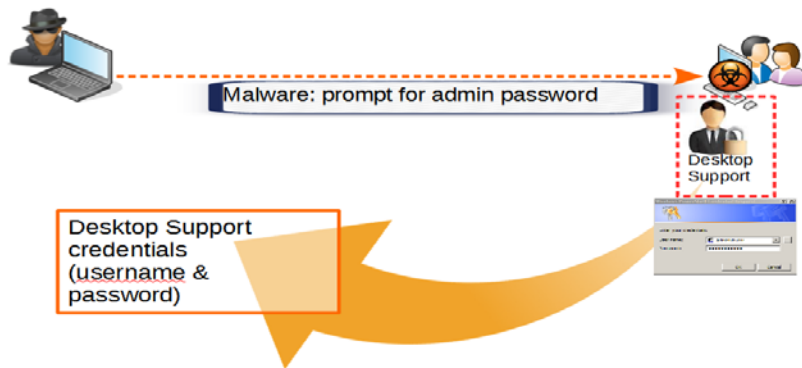
During the scan, approximately 30 physical security cameras were found and accessible through HTTP/HTTPS. Password guessing, along with user manuals for each make and model of camera, allowed the Team to identify default passwords on numerous devices. The user manuals, along with most tools used by the team are readily available on the Internet. In several instances the administrator account/password combination was the same allowing administrator level access to the camera. Administrator access allowed the attackers to change the direction the camera was pointed, change the focus, reboot the camera, record, and open/close the shutter.

Other default administrator account/password combinations were found for:

- A legacy PBX system
- 3 Quantun Scalar backup systems
- A power meter
- IP-enabled audio codecs
- A barcode device
- A DS3 device

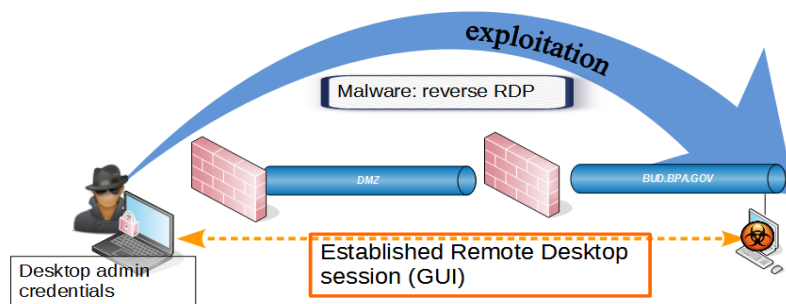
Also found was an Integrated Lights-Out-Management (iLOM) device with “emergency admin password bypass” enabled. This feature allows an attacker to reboot the machine with a custom operating system.

Exploitation



Then the attackers concentrated on privilege escalation. During the password guessing activity the team was unsuccessful in acquiring the password to an "epu" account. As a result, the attackers decided to "force" the owner of an "epu" account to enter their password. Again using the LDAP listing of accounts and groups, the attackers identified a group described as "*Resource: Grants Administrative access to all non-exempted BPA workstations*". Next, the group utilized the command-line tool "dsquery.exe" (installed on the Citrix server "Shared Desktop 7") to list the users in this group. This activity allowed the attackers to identify elevated accounts following the format "epuDO". A comment was found that associated epuDO accounts with a function, "Help Desk and Outreach – Portland". This identified a link to the Help Desk function for internal.bpa.gov. The attackers then wrote a script that would not allow a user's desktop to appear until a valid "epuDO" account was typed in. The script was placed on one of the desktops on which the phishing attempt was successful previous in the operation. The Team killed a process on the machine and that allows interaction with the desktop by the user, the script killed the process called "explorer.exe" continuously until valide domain elevated privilege account (EPU) credentials were provided and captured by the software and sent an email to the Team letting them know it was successful. The script was successful and a valid "epuDO" credential was captured giving the attackers administrative rights on the majority of BPA workstations.

Installation and C2



Utilizing the previous phished connection, the team uploaded executables enabling them to forward RDP sessions outbound back to their Command and Control (C2) servers. Using this “reverse RDP” technique, they were able to remote-desktop to other workstations and servers.

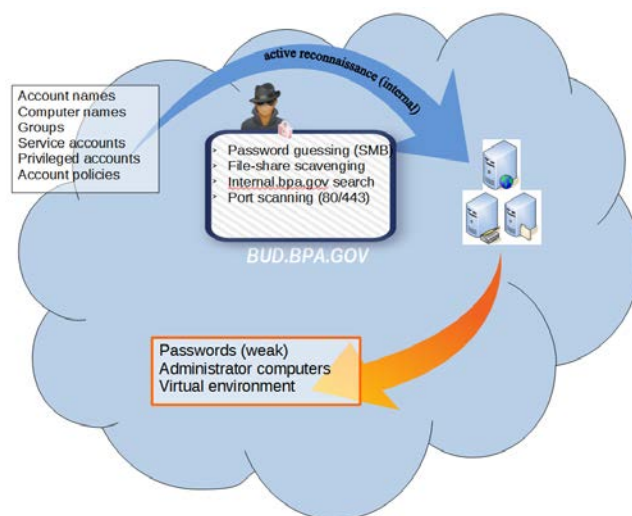
Additional discovery’s included:

- Citrix Web Interface
- Link to “Shared Desktop 7” which connected to a Windows 2003 Server in a 32-bit Citrix environment. This environment had MSOffice 2003 and other legacy software. User Access Control (UAC) elevation is not required and allowsthe“RunAs” command.
- For “epu” accounts, a link to “Nova Desktop” providing a Windows 7 64-bit environment in a Citrix environment.
- The “MyPC.bud.bpa.gov” also providing a Windows 7 64-bit environment.

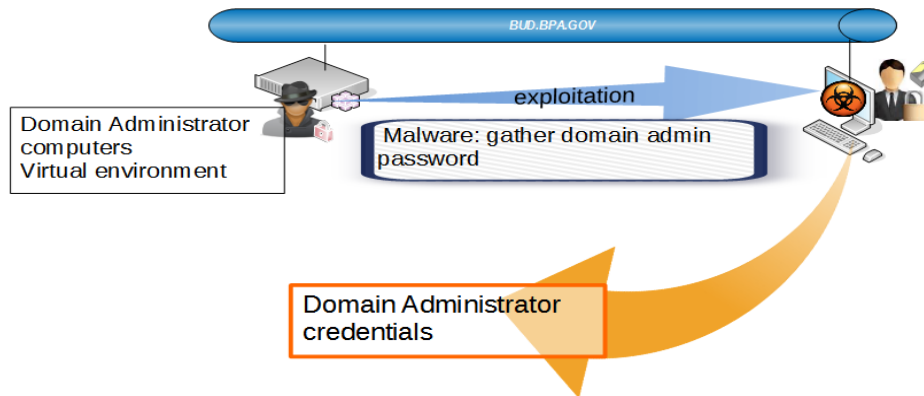
Action on Objectives

The new found access allowed the attackers to begin lateral movement, from the BUD network, into other, into anywhere that appeared to be mission critical environments such as the Control Center Network (CCN) and the Field Information Network (FIN).

Finally, the team began working on obtaining the credentials to at least one domain administrator. Referencing the previously obtained LDAP listing, they identified all accounts with the format “epuAD”, cross referenced these individuals with the workstations to identify the machines used by Domain Admins. The assumption was the administrators would use both their regular accounts and their admin accounts from the same machine.

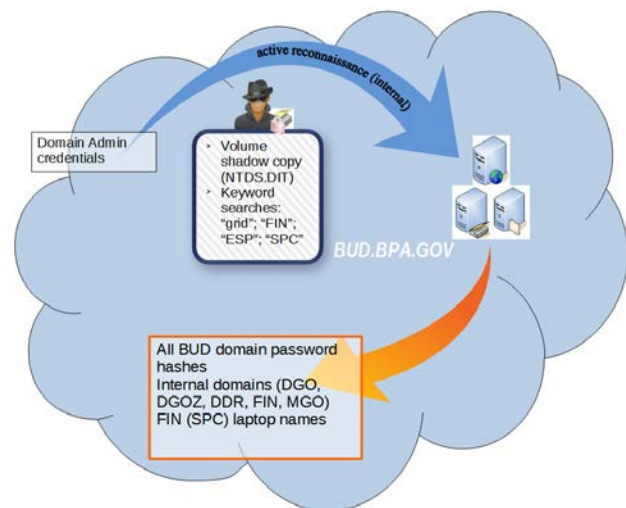


Exploitation



The attackers used the Microsoft SysInternals tool “PsExec” to run “Mimkatz” on all workstations used by domain administrators resulting in credentials for all domain administrators. “PsExec” is commonly used by Windows system administrators so the use of it in logs would not raise suspicion. Additionally, it would not be blocked by protection software. “Mimkatz” captures, in clear text, the credentials of any account that was authenticated on the server since last boot.

Now the attackers had the credentials to Help Desk and Domain Administrator accounts. The attackers used the “set” command from the Windows command-line to find the “LOGONSERVER” environment variable of one of the original phished accounts. This provided the name of the domain controller. Using the domain administrator’s credentials, the attackers were able to run Windows’ “volume shadow copy” process on the domain controller. This process secured the NTDS.dit file from the domain controller. Using the Linux-based “SMBToolkit”, dumped the password hashes for all accounts on the domain. The attackers assumed an eight character password that started with a capital letter followed by a lowercase letter and all combinations for the remaining six characters (e.g. “Seattle1”). Using this mask the team began trying to crack those hashes to obtain their plain-text passwords. The result, over 10% of the BUD domain fell in four days.

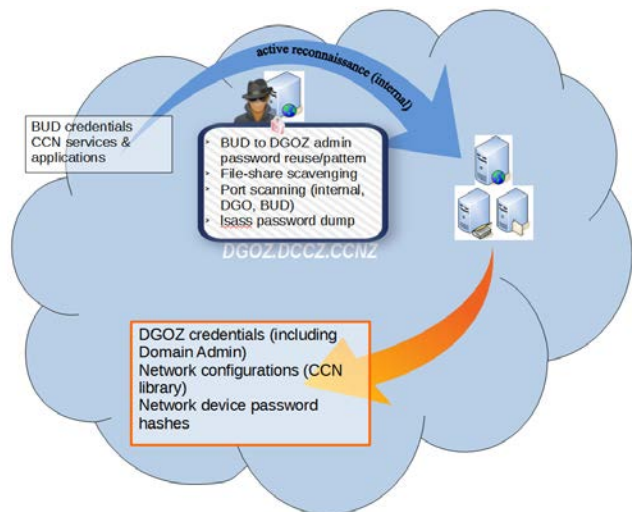


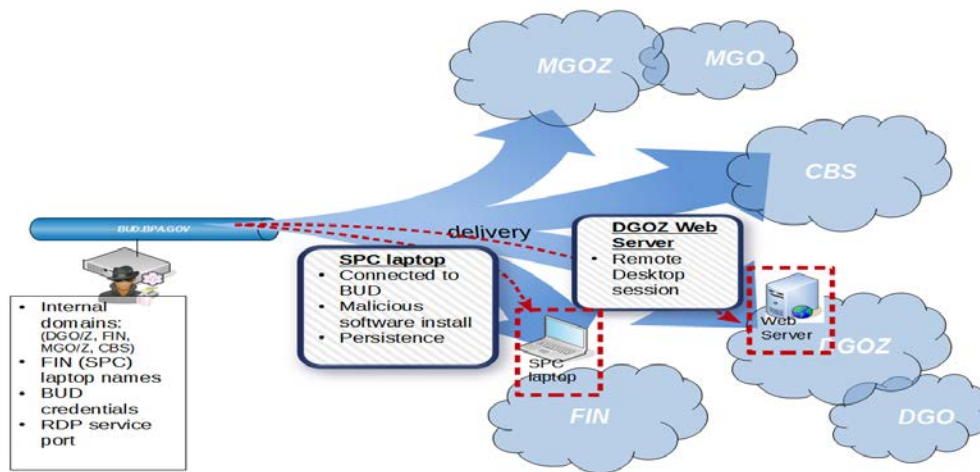
Internal Activity on other BPA networks

Armed with usernames and passwords, the attackers again began active reconnaissance using remote desktop into MyPC and “Nova Desktop” as those users. The search criteria entailed anything containing the phrase “the grid”. The results included documents discussing the Field Information Network (FIN) and the Control Center.

Based on the information obtained up to this point, the attackers decided to attempt to “own the domain”. The thought was once they had Domain authority to all of the BPA environments, they could selectively target any organization or individual.

Internal reconnaissance had turned up a document that pointed to the existence of 4 domains named DGO, DGOZ, MGO, and MGOZ. Relatedly, the attackers had previously searched internal.bpa.gov for the terms "BUD" and "Active Directory" and one of the search results was a document titled "IT Wiki - DNS Topology for BUD and ADR Domains". This document displays a breakdown of the DNS interconnections within BUD. One of the elements listed in this diagram under ADR.BPA.GOV Domain (Forest Root) were conditional forwards to DCCZ.CCNZ and GTS.CBS. This information, combined with previous information, provided the attackers with evidence that CBS was called "Critical Business Systems", and it had its own domain, GTS.CBS. The attackers' attempts to infiltrate GTS.CBS using previously obtained credentials, was not successful.





Field Information Network (FIN)

Active reconnaissance

Results from document searches included documents pertaining to the FIN such as one titled "Regular Access procedure". This document described how to connect a device on the (b) (5)

Again using the LDAP dumps, the attackers found approximately 113 machines with "SPC ATG 32bit" in the description and whose names ended in "WIN7". Looking up "SPC ATG" on internal.bpa.gov brought us to the "Dell ATG Wiki" page. Included in the links on the Dell ATG Wiki, was a link which appeared to show a phone test set and Serial-to-USB cables next to one of these laptops. Since Serial-to-USB cables are usually used to connect to non-networked equipment (such as field equipment), the attackers suspected the laptops pictured were in fact the SPC laptops found in the LDAP queries.. Using the information gathered so far - knew they were Dell ATG laptops - the attackers searched the Dell website for "Dell ATG" and found that these are "semi-ruggedized laptops for outdoor environments".

A simple ping sweep of the 113 SPC ATG laptops found in the LDAP dumps, the attackers found that about half of the 113 "SPC ATG" laptops are connected to the BUD network at any given time.

Weaponization

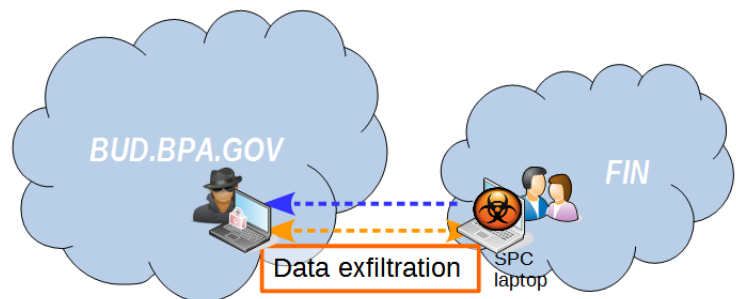
Suspecting the field workers may use these machines to log into SCADA equipment when not on BUD, the attackers created malware that would run autonomously on these SPC laptops and not require a network connection.

Delivery and Installation

While the SPC laptops were connected to the BUD domain, the malware was placed on the victim machines through the Microsoft PSExec tool using a BUD Desktop Administrator account.

Exploitation and Actions on Objectives

The malware captured screenshots of the SPC laptop's desktop every 10 minutes (for any user that logged in), detected if the SPC laptop was on BUD or not, notified the attackers when the laptop was plugged into BUD again, and uploaded the pictures and network information files to the



attackers' C&C server on the Internet. The attackers then analyzed the screenshots to see which workstations actually touched field equipment. The attackers obtained screenshots of users as they were logging into Sequential Event Recorders (SER), ABB Line Distance Protection Terminals (REL-531), General Electric D400 Substation Gateways (D400), Schweitzer Engineering Laboratories Phase and Ground Distance Relays (SEL-321), and Schweitzer Engineering Laboratories Protection, Automation, and Control Systems (SEL-421). The screenshots were taken when the users were on FIN and also when they weren't connected to any network at all.

While looking at the screenshots, the Team also analyzed the accompanying network information files and found that the FIN network has a Fully Qualified Domain Name called "FIN.BPA.GOV". For the most part, the FIN appears to be separate from BUD, but one of the network information files showed that the user could traceroute to www.google.com while only being connected to the FIN network.

The attackers were able to guess the BUD password for a user account belonging to a foreman in Montana. When the attackers logged into BUD using this account and scoured the foreman's file shares for any file with the word "password" in it, they found a document that contained Level 1

(b) (5)



Control Center Network (CCN)

Active reconnaissance

While running PsExec on a remote workstation, an error message popped up that listed an address in a domain labeled DGOZ.dccz.ccnz. Leveraging internal reconnaissance, it was learned that DGOZ is a DMZ domain between BUD and something called the Control Center Network (CCN). Documentation also showed that inside the DGOZ, they had changed the Remote Desktop TCP port to 15001, instead of the default 3389. This, along with the naming convention of the 4 domains, also led the attackers to believe that the DGO network was being protected from the BUD network by the DGOZ, and probably the MGO network was being protected from BUD by the MGOZ.

Using a captured BUD user account, the attackers started information mining mapped files shares associated with the user's account. The file share turned out to be a central repository for CCN information (ccnlibrary). Documentation in this share provided IP addresses for servers located within the DGOZ DMZ, pointing to the 10.193.x.x subnet as the range of addresses utilized.

Actions on Objectives (lateral movement)

Using the information discovered about the DGOZ, the attackers created a rudimentary port scanner on MyPC (using PowerShell) and found that they were able to connect to remote desktops on many DGOZ machines from BUD. This was possible because several DGOZ accounts were found to have the same username/password combination in the DGOZ domain. Further, a domain admin was identified that appeared to use a pattern in their BUD password; modifying this pattern ultimately led to guessing the password for the corresponding DGOZ domain admin account. Some of the DGOZ accounts had local administrator rights on servers in the DGOZ, with which the attackers were able to modify webpages of DGOZ internal websites and gain full access to an internal file server.

Active reconnaissance

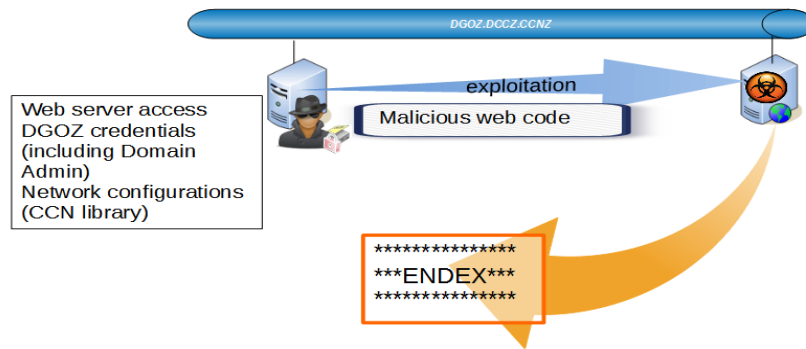
According to the DGOZ/DGO network maps, no traffic was allowed directly into DGO from DGOZ, and port scans subsequently verified this. Looking at the IIS web logs for the servers, it appeared non-DGOZ workstations were logging into some of the web servers in DGOZ.

The attackers began exploring common shares (like the ccnlibrary) with the newly compromised accounts, and by logging in as network administration staff, the attackers were able to locate several network configurations. Some of these network configurations contained Cisco Type 7 password hashes that allowed the attackers to uncover a password that may be reused throughout the environment. As well, multiple versions of the Cisco IOS are in use, many of which appear vulnerable to attack. However, the CISO advised against modifying network devices, so this pathway was abandoned.

Weaponization

At this point, the attackers determined the best avenue for getting into DGO was to try another social engineering attempt. The attackers considered uploading a malicious Java applet to one of the websites in the DGOZ web servers, but were unable to determine if DGO workstations had Java installed. As it was reasonable to assume the workstations in DGO had Microsoft Office installed, the attackers decided to use a malicious Excel file again. The malicious Excel file was to be uploaded to the DGOZ file server, and then the main page of one of the web servers modified to prompt the user to open this Excel file.

End of Exercise



During the planning phase of attacking DGO, personnel in DGOZ stumbled on a modified file (JB.aspx.txt) and contacted Cyber Security to see if the group was responsible for its presence.

At this point the attackers had successfully infiltrated, from BPA HQ, to the Control Center DMZ (a sub network that contains and exposes external-facing services to the business administrative networks and in turn the Internet). The entire Active Directory Domain was controlled by the attackers. Additionally, the attackers were performing actions, in line with the cyber kill chain, to launch an attack against the core of the Control Center. The attackers were detected completely by accident. The detection was not reported and the incident response process was not exercised.

At this point, the CISO terminated the exercise.

Recommendations

(b) (5)

[Redacted content]

Appendix A: Definitions

FIELD INFORMATION NETWORK (FIN) - BPA network used for remote access to Critical Cyber Assets in substations and other field locations.")

LATERAL MOVEMENT - moving from workstation to workstation, workstation to server, server to server, etc. within the network.

PHISHING - Email attempt to acquire sensitive information.

SPEAR PHISHING - An email spoofing fraud attempt that targets a specific organization seeking unauthorized access to confidential information

SPOOFING - the masquerade of one individual as another by falsifying data and thereby gaining illegitimate advantage.