# Precision Widgets of North Dakota Attack

## Incident Report

**Paul Corapi, Connor McDonald, Charles Wasaff**

**April 2020**

**Table of Contents:**

# 1. Background

Precision Widgets of North Dakota (PWND) is a manufacturer of high-tech precision aircraft and mobility parts primarily for government customers across the globe. PWND owns patents for several processes and designs which are the foundation of their brand and their most precious asset.

PWND was recently outbid on a contract to manufacture 150,000 Rascal scooter performance exhaust systems for the local government of Fort Lauderdale Florida. Due to PWND's previous success in this area and substantial cost advantages in the market PWND's CEO and founder Billy Honeydew immediately suspected that they could have mean a victim to theft of their intellectual property.

Our team consists of Paul Corapi, Connor McDonald, and Charlie Wasaff. We are incident response consultants from Johnson and Johnson and Johnson LLP tasked with discovering if there was data stolen from the PWND network, and if so how. Our team worked on this investigation from 4 March to 9 April 2020.

# 2. Findings

### 2.1 Major Findings

- *Major Finding 1*: The attackers extracted 55 files, including the file “Intellectual Property” from PWND computers.
- *Major Finding 2:* The attackers initiated the penetration of PWND information infrastructure via the social media website Twitter.

### 2.2 Evidence examined

- Disk Images from PWND CEO, PWND Administrator, and another PWND computer
- PWND network traffic capture
- PWND CEO Billy Honeydew’s Twitter Account
- Attacker Twitter Account, *@mystry_strngr*

# 3. Timeline

| Time | Event | Source |
|---|---|---|
| 05/01/2017 07:54 | Initial Malware Delivery | |
| 05/03/2017 01:16 | Payload downloaded on PWND-CEO | Pwndceoiehistory.txt from volatility showed his internet explorer history. |
| 05/03/2017 01:19 | PWND-CEO connects to C2 | Pwnceonetscan.txt which was captured from the tool volatility. |
| 05/03/2017 02:06 | Payload transferred to 192.168.64.137/PWND-ITADMIN | |
| 05/03/2017 02:11 | PWND-ITADMIN connects to C2 | Pwnditadminnetscan.txt which was captured from the tool volatility. |
| 05/03/2017 02:16 | Payload transferred to 192.168.64.149/PWNDDC01 | Pwnddc01.pcapng containing captured network traffic. |
| 05/03/2017 02:20 | Pwnddc01 connects to C2 | Pwnddc01.pcapng containing captured network traffic. |

# 4. Analysis Details

### 4.1 Reconnaissance

The first part of our analysis examines the reconnaissance phase of an intruder attack. As a part of this reconnaissance, the intruder needed to identify the internal network and IP addresses of key computers, as well as any other information that they could easily gain online. During this analysis we found the internal IP addresses of the key computers within the PWND network using a variety of tools, including *netscan*. The IP address of PWND-CEO was found to be 192.168.64.136, the PWND-ITADMIN has an IP of 192.168.64.137, and PWNDDC01 has an IP of 192.168.64.149. The intruder also had access to Billy Honeydew's Twitter, *@PWND_BHoneydew*. It appears that the intruder used the Twitter account *@mystery_strngr* to contact Billy Honeydew for reconnaissance. This information was found using the *Volatility* tool on PWND-CEO's Internet Explorer history. The link to the malware is the following: *http://precisionwidgetsnorthdakota.com/PrecisionWidgets.bat*. Other information found in the reconnaissance was an active time bias of 240 on the PWND-ITADMIN account, meaning that the time zone was Eastern Daylight Time.

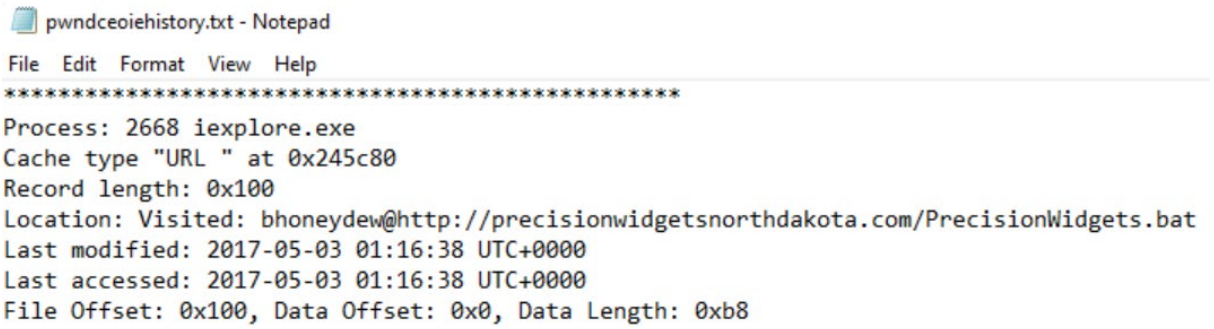


Fig. 4.1: Image of PWNDCEO visiting the location of the malware.

**4.2 Delivery**

The malware was initially delivered at 07:54 on May 1, 2017. However, the malware's payload was not downloaded on the PWNDCEO user until 01:16 on May 3, 2017. This means that there were 2 days between the initial delivery and when it accessed PWNDCEO.

**4.3 Weaponization**

The type of malware was found to be *windows/meterpreter/reverse_http.*

**4.4 Command and Control**

From our analysis we found that the malware was using a C2 server with the IP address 138.68.64.108. The malware connected to this website using the destination port 4443 which uses TCP as its protocol. PWNDCEO first connected to the C2 server at 01:19 on May 3, 2017. This is approximately 3 minutes after the malware was downloaded to PWNDCEO's account. In total, 23142 packets were sent between PWNDCEO and the C2 server. The C2 server also connected to PWNDITADMIN and PWNDDC01 at 02:11 and 02:20 respectively on the same date. These times were both 4 to 5 minutes after the malware was downloaded on each account as outlined below in the Action on the Objective section.

**4.5 Installation**

After a careful review of event logs and some thorough memory analysis, we have discovered that the malware was running on the system under the PID 1708, as this process is revealed through the Volatility plugin *malfind*, a plugin which identifies injected or hidden code in memory, when run on the PWND-CEO machine. Here, the '*4d5a'* 2-byte hex string indicates that the process has injected code intended to be executed.

```
Process: TPAutoConnSvc. Pid: 1708 Address: 0xe10000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 111, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00e10000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x00e10010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x00e10020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00e10030  00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00   ................
```

Fig. 4.5.1: Injected byte hex string

We know that this malware came from the internet because of the "Zone Identifier" data stream associated with the file, which assigns a number to the file based off of where it originated, in this case being the Internet, or a 3. After decoding the payload instructions from the downloaded file, we discovered it was instructing the host machine to download the data from *http:///138.68.64.108:4443/$n*, which is the IP address of the C2 server combined with the port/protocol the malware was utilizing to communicate between the host machine and that server.

On the PWNDITADMIN machine, we discovered a process that had injected executable code within it, again identifiable from the 2-byte hex string within its hex code '*4d5a'*. The process was *TPAutoConnSvc.exe* and appeared in the *malfind* Volatility plugin when run on the PWNDITADMIN machine.

```
Process: TPAutoConnSvc. Pid: 1716 Address: 0x1c40000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 301, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x01c40000  4d 5a 41 52 55 48 89 e5 48 83 ec 20 e8 00 00 00   MZARUH..H.......
0x01c40010  00 5b 48 81 c3 af 1e 00 00 ff d3 48 81 c3 40 03   .[H........H..@.
0x01c40020  12 00 89 3b 49 89 d8 6a 04 5a ff d0 00 00 00 00   ...;I..j.Z......
0x01c40030  00 00 00 00 00 00 00 00 00 00 00 00 01 00 00      ...............
```

Fig. 4.5.2: Identified 2-byte injection string '*4d5a*'

Additionally, we discovered that the hacker used his connection with the PWNDITADMIN machine to upload a 2916-byte file which, given the times for when the file was created, accessed, and modified, was most likely put on the PWNDITADMIN machine with the *copy* file operation.

**4.6 Actions on the Objective**

In all, the extent of the data that was transferred from the system it was exfiltrated from was roughly 11MB. In order to properly stage for the exfiltration, the hacker used the tool named *7.exe* which is stored in the PWND-CEO machine's root directory. The original name of the staging tool was *7za.exe*, as you can see by browsing to the 'Details' tab of the "Properties" window that you can arrive at from the context menu of the file in Browser.

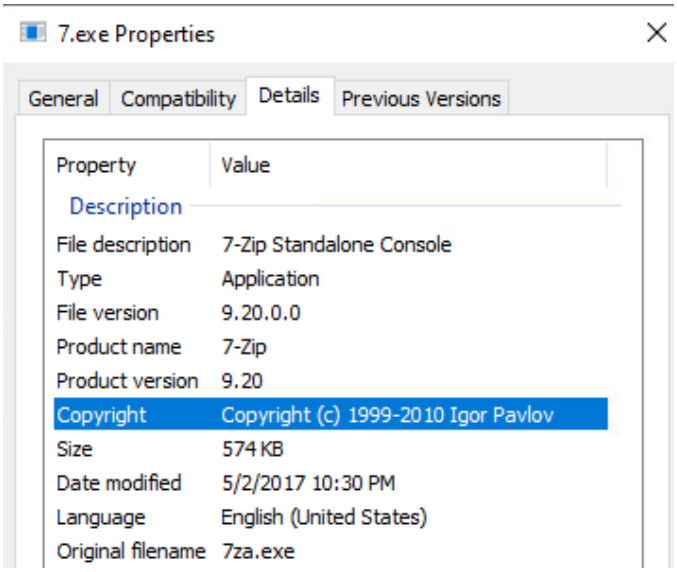


Fig. 4.6.1: Original name of staging tool.

The attacker renamed the staging tool to *USERSBHONEYDEW7.EXE* before changing it back to *7ae.exe*. The attacker tried to run commands as the administrator and in turn caused the domain credential to be stored in memory (*runas /user:pwnd\pwnddc01 cmd*). Attackers will run commands as the administrator in order to attempt lateral movement, much like this attacker did. The attacker then transferred a batch file named *prec.bat* between machines on the network (laterally) using the Server Message Block ("SMB") protocol to two machines on the network. The first machine (IP address 192.168.64.137) at 0206 and the second machine (IP address 192.168.64.149) at 0216, both on May 3rd, 2017. The laterally transferred batch file was executed via the Windows Management Instrumentation's command-line utility, *WMIC*. The attacker left artifacts that enabled us to gain access to their Twitter account with the password "SecretPass123." In total, the attacker exfiltrated 55 files, of which the most concerning exfiltrated file was titled "Intellectual Property."


Fig 4.6.2: Access inside malicious Twitter account, @mystery_strngr