

Incident Analysis Report

Group 2



June 22, 2019

Phenomenoc-DC

***Raghda Yousef***

***Marwan Reda Ramadan***

***Abdelrhman Kamal***

***Mohamed Nabil***

***Ahmed Mohamed***

**Incident Analysis Report: Domain Controller LAN Segment**

**LAN Segment Details:**

* **Range:** **10.0.76.0/24** (**10.0.76.0** through **10.0.76.255**)
* **Domain:** **phenomenoc.com**
* **Domain Controller:** **10.0.76.6** - **Phenomenoc-DC**
* **Gateway:** **10.0.76.1**
* **Broadcast Address:** **10.0.76.255**

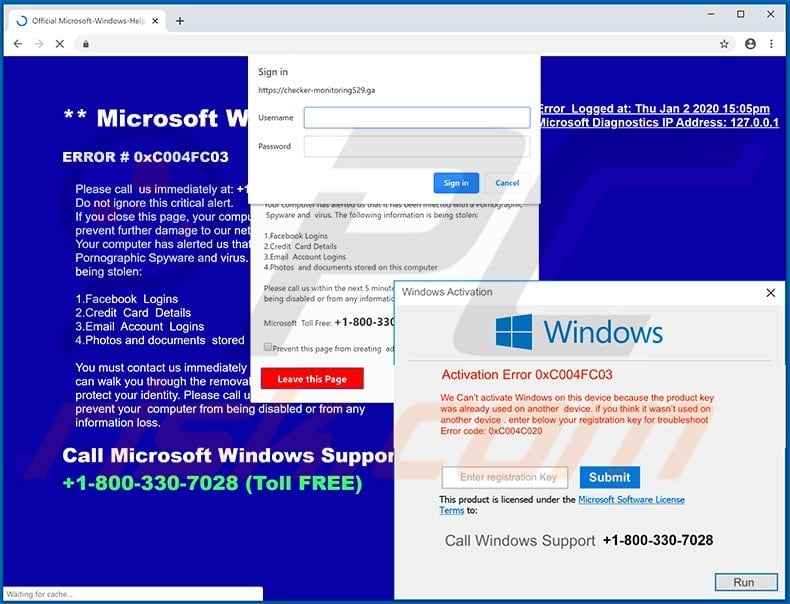
### **Key Findings**

1. **Infected Windows Host Details:**
   * **IP Address:** 10.0.76.109
   * **MAC Address:** 78:2b:cb:d4:a5:fe
   * **Host Name:** BANGKOK-8AC2-PC
   * **Windows User Account:** edris.haight
2. **Malware Delivery Method:**
   * Exploit Kit: **REG Exploit Kit (REG EK)**
   * Initial access achieved when the victim visited a malicious website named **letsdoitquick**.
   * The website permanently redirected traffic to **37.46.135.170**, where a trojan payload was delivered.

A screenshot of a computer

Description automatically generated**2.1.(redirect from lets do it quick to 37.46.135.170 )**

**A screenshot of a computer

Description automatically generated2.2.** **Trojan.Cryxos is a type of malware primarily used for social engineering attacks, often masquerading as fake security warnings or technical support scams,its may redirect user to download or give attacker sensitive data to get explit through toolkit**

A screenshot of a computer

Description automatically generated2.3.**Adobe Flash** was exploited as part of the REG EK tactic using **CVE-2018-4878**, resulting in the download of the executable file **KPOT Stealer**.

A screenshot of a computer

Description automatically generated

2.4.download of the executable file **KPOT Stealer this request come from script agent** .

A screenshot of a computer

Description automatically generated(We found user agent come from scripting environment this is malware script download this exe file)

**3.Malware Details:**

**Malware Type:** KPOT Stealer

**Executable Behavior:**

-When executed, the EXE persists itself in C:\Users\admin\AppData\Local\Temp\Rar$EXb6360.20748\2019-06-22-malware-retrieved-from-the-infected-Windows-host.exe

-This malware check HKEY for security policeis to may be gather browser information like cookie and autofill password .

-The EXE deletes itself after completing its mission.

-Establishes a connection with **fghjkmgru34.site**.

**Executable Hash (SHA256):** 39be5610259ffade85599720ee0af31187788a00791f1e4cb0cd05ef00105eda

**Post-Infection Traffic:**

**IP Address:** 8.209.83.76

A screenshot of a computer

Description automatically generated**Domain Name:** fghjkmgru34.site

**4.Second Windows Host Details:**

**IP Address:** 10.0.76.193

**Activity Analysis:**

-The user visited various legitimate websites, including **beef2live**.

-A significant number of alerts were generated due to normal tracking systems employed by websites (e.g., Google Analytics) and activities involving plugins and small-sized GIFs.

**A screenshot of a computer

Description automatically generatedConclusion:** No suspicious activity detected. User activity deemed normal.

### **Incident Timeline**

1. **Initial Access:**

**Victim Host (10.0.76.109)** visited **letsdoitquick**, leading to a redirection to malicious IP **37.46.135.170**.

1. **System tricking:**

**Trojan.Cryxos** performed reconnaissance to gather system details, including OS, browser version, and installed software.

1. **Tailored Exploit:**

Based on fingerprinting data, the attacker triggered a fake Adobe Flash update exploiting **CVE-2018-4878** (a remote code execution vulnerability in Adobe Flash Player).

1. **Final Payload:**

The exploit installed **KPOT Stealer** (SHA256: 39be5610259ffade85599720ee0af31187788a00791f1e4cb0cd05ef00105eda), a credential/data-stealing malware.

1. **Post-Infection Traffic:**

Exfiltration of sensitive data was conducted over **8.209.83.76** using the domain **fghjkmgru34.site**.

1. **Observations Regarding Host 10.0.76.193:**

A screenshot of a computer

Description automatically generatedUser activities included accessing legitimate websites like **beef2live** and interacting with tracking systems (e.g., Google Analytics).

### **Technical Analysis**

1. **Delivery Mechanism:**
   * The REG EK exploited vulnerabilities in Adobe Flash to execute malicious payloads.
2. **Payload Behavior:**
   * **KPOT Stealer** extracted sensitive information (e.g., credentials, browsing history).
   * Persistence was achieved by storing the EXE in C:\Users\admin\AppData\Local\Temp\Rar$EXb6360.20748\2019-06-22-malware-retrieved-from-the-infected-Windows-host.exe
   * A screenshot of a computer

     Description automatically generatedA screenshot of a computer

     Description automatically generatedfollowed by self-deletion post-mission.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

**3.Post-Infection Traffic:**

* + Communication with command-and-control (C2) server at **8.209.83.76**.

### **Recommendations**

1. **Immediate Actions:**
   * Isolate the infected host (10.0.76.109) from the network.
   * Block access to malicious IPs (37.46.135.170, 8.209.83.76) and domains (letsdoitquick, fghjkmgru34.site).
2. **Remediation Steps:**
   * Perform a full malware scan on the infected host.
   * Remove KPOT Stealer and other associated malicious files.
   * Reset all credentials potentially compromised.
3. **Preventive Measures:**
   * Update all systems and applications to the latest versions to patch vulnerabilities like CVE-2018-4878.
   * Employ advanced endpoint protection with behavior-based detection.
   * Monitor network traffic for unusual activity and implement intrusion detection/prevention systems.
4. **User Awareness:**
   * Educate users on avoiding malicious websites and recognizing phishing attempts.

### **Conclusion**

This incident highlights the exploitation of outdated software and user behavior as primary attack vectors. Effective patch management, user training, and advanced threat detection mechanisms are critical to preventing similar attacks. The rapid identification and isolation of the infected host mitigated further damage within the domain controller LAN segment.