FIDELIS CYBERSECURITY

www.fidelissecurity.com
www.threatgeek.com
@FidSecSys
+1800.652.4020

Fidelis Threat Advisory #1017

Phishing in Plain Sight

June 9, 2015

```
Document Status:   FINAL
   Last Revised:   2015-06-08
```

Executive Summary

Fidelis Cybersecurity analysis has identified unrelated cyber criminal activity leveraging the vulnerability cited in CVE-2014-4114, which was initially exploited by advanced persistent threat (APT) actors in October 2014. Notably, some of this recent activity demonstrated actors implementing a technique that bypassed antivirus detection by saving a PowerPoint document in which malware executed once the document was opened in Slide Show presentation format. The identification of cyber crime actors, particularly Nigerian 419 scam operators, attempting to exploit CVE-2014-4114 demonstrates how quickly cyber criminals are trying to exploit a vulnerability previously associated with espionage actors, using similar tactics, techniques, and procedures (TTP) to maximize their chances of success, with additional innovation as seen with these samples.

Key Findings

- We identified threat actors using weaponized PowerPoint documents that exploited CVE-2014-4114 to create an executable dropper that entrenched different malware in the victim system based on the actor's choosing.
- In order for the exploit to trigger, the malicious document must be opened in Slide Show presentation format (e.g. PPSX or PPS or by selecting to view the document presentation mode from PowerPoint). We observed that the adversary is saving the document in PPS format in order to bypass all antivirus detection. See APPENDIX B for more details.
- Based on our observations, multiple seemingly unrelated cyber crime campaigns of varying sophistication levels are targeting the CVE-2014-4114 vulnerability. We believe

While we have done our best to ensure that the material found in this document is accurate, Fidelis Security Systems, Inc. makes no guarantee that the information contained herein is error free.

that cyber criminals, particularly Nigerian 419 actors, are now seeking to exploit vulnerabilities first leveraged by espionage actors. If true, this would represent an evolution in 419 actor TTPs from previous operations.

Threat Overview

Recent Fidelis Cybersecurity analysis uncovered seemingly unrelated cyber criminal activity of varying sophistication levels seeking to exploit the vulnerability cited in CVE-2014-4114. Many of these incidents involved spearphishing and included weaponized PowerPoint attachments that claimed to be a “purchase order.” Further analysis revealed other incidents that implemented the same Custom Information File (.INF) found in the malicious documents that Fidelis Cybersecurity was investigating. The title, author and creation date properties of this document were the same suggesting the same author had compiled the exploitation kits using different PowerPoint attachments than was originally implemented in the 2014 activity. More importantly, we identified threat actors using weaponized PowerPoint documents that exploited the CVE-2014-4114 to create an executable dropper that entrenched different malware based on the actor’s choosing in the victim system. We observed that the adversary is saving the document in PPS format in order to bypass all antivirus detection.

For technical analysis of the malware associated with this activity, see APPENDIX A.

For technical analysis of how the weaponized PowerPoint evaded antivirus detection, see APPENDIX B.

What’s Special About CVE-2014-4114?

The recent spearphishing events targeting CVE-2014-4114 elicited attention due to the history of the previously unknown vulnerability’s initial discovery and the suspected nation state-affiliated actors behind the original activity.

According to the National Vulnerability Database, unpatched versions of Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2 and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted OLE object in an Office document, as exploited in the wild with a "Sandworm" attack in June through October 2014, aka "Windows OLE Remote Code Execution Vulnerability."[i]

“Sandworm Team”

In late 2014, a private security vendor worked with Microsoft to announce the discovery of a zero-day vulnerability impacting all supported versions of MS Windows and Windows Server 2008 and 2012. Exploitation of this vulnerability was discovered in the wild in connection with a cyber-espionage campaign that the security vendor attributed to Russia, based on spearphishing assets related to the North Atlantic Treaty Organization, foreign government and military organizations, energy and telecommunications companies, as well as geopolitical considerations. In many of the 2014 incidents, a weaponized power point was implemented.[ii]

Not the Same Actors

While there are superficial similarities between the original 2014 incidents exploiting CVE-2014-4114 and the recent 2015 events, Fidelis Cybersecurity does not believe the original actors, suspected of being nation state-affiliated, are involved. The tradecraft involved in most of the recent CVE-2014-4114 activity is more similar to various cyber criminal actor sets than nation state-affiliated actors based on various levels of social engineering tradecraft and in some instances, the use of malware methods that bypass antivirus program detection. Notable distinctions between the 2014 and 2015 spearphishing e-mail campaigns include but are not limited to:

- **Social Engineering Tradecraft**. Social engineering observed in the 2015 campaigns has ranged from poorly constructed e-mail messages with multiple misspellings and poor grammar to more polished language. Additionally, e-mail content – the desired purchase of unidentified merchandise or services – did not correspond to the position and title of the individual to whom the e-mail was sent. Suspected nation state cyber espionage actors typically are more careful about how e-mails are crafted and the content they carry to maximize the opportunities for the targeted individuals to click on the hostile link or attachment.
- **PowerPoint Attachments**: The actual PowerPoint attachments observed in the 2015 activity were not topically tailored to entice the recipient into opening them. In contrast, the 2014 activity featured legitimate, albeit weaponized, attachments the content of which would be relevant to the recipients.[iii]

A Nigerian Connection

In some of the observed 2015 activity, there is strong circumstantial evidence indicating that Nigerian 419 actors are involved in part of this overall activity trying to exploit CVE-2014-4114. Many of the same TTPs bore striking similarities to similar Nigerian activity in 2014. If true, this is a notable evolution in traditional Nigerian 419 fraud operations. For more connections to Nigeria attribution, see APPENDIX C.

- **Nigerian Operations.** Since 2014 there have been indications that Nigerian actors have evolved their 419 fraud scams.[iv] In many of these instances, these actors have implemented such tools as Netwire RAT and DarkComet RAT, among others. One campaign cited suspected Nigerian actors engaged in APT-like activities targeting oil transportation tankers aiming to siphon off credentials and data. [v]

- **"Gozie Brinkley."** Another circumstantial data point that potentially links the April 30 incident to Nigerian actors is the name "Gozie Brinkley," which was found in the malware string. Open source research associated with that name brings up several Nigerian-related results, particularly a Facebook profile that advertises "Free SMS, Tunnel Guru" intimating that this individual knows how to leverage cellular networks.

Indicators and Mitigation Strategies

Rules to detect some of the threat observed during this research

- Netwire RAT – File detection rule using Yara

```
rule crime_win32_exe_rat_netwire{
  meta:
       Copyright = "Fidelis Cybersecurity"

       hash = "fd5a753347416484ab01712786c407c4"
   strings:
       $sa = "StubPath"
       $sa = "CONNECT"
       $sa = "200 OK"
       $sa = "GET"
       $sa = "Host"
       $sa = "Connection"
       $sa = "Firefox"
       $sa = "Chrome"
       $sa = "Opera"
       $sa = "Outlook"
       $sa = "NSS_Shutdown"
       $sa = "NSSBase64_DecodeBuffer"
       $sa = "NSS_Init"
       $sa = "NSS_Shutdown"
       $sa = "name" nocase
       $sa = "password"
       $sa = "Server"
       $sa = "LANMANNT"
       $sa = "SERVERNT"
       $sa = "[Backspace]"
       $sa = "[Enter]"
       $sa = "[Tab]"
       $sa = "[Print Screen]"
       $sa = "mozsqlite"
       $sa = "nssutil"
       $sa = "sqlite"
       $sa = "Email"
       $sa = "POP3 User"
       $sa = "POP3 Server"
       $sa = "POP3 Password"
       $sa = "IMAP User"
       $sa = "IMAP Server"
       $sa = "IMAP Password"
       $sa = "HTTP User"
       $sa = "HTTP Server"
       $sa = "HTTP Password"
       $sa = "SMTP User"
       $sa = "SMTP Server"
       $sa = "SMTP Password"
   condition:
      (uint16(0) == 0x5A4D) and (all of them)
}
```

- Information Stealer – Network traffic detection through the use of regular expressions against the URL

```
\.php\?type=clipboard&machinename=(.*?)&windowtitle=(.*?)&clipboardtext=(.*?)&machinetime=

\.php\?type=notification&machinename=(.*?)&machinetime=
3.   \.php\?type=keystrokes&machinename=(.*?)&windowtitle=(.*?)&keystrokestyped
     =(.*?)&machinetime=

4.   \.php\?type=passwords&machinename=(.*?)&application=(.*?)&link=(.*?)&usern
     ame=(.*?)&password=
```

For a more comprehensive list of technical indicators, see APPENDIX A.

Mitigation Strategy

Enterprises are reminded to apply security updates to all applications and systems in a timely manner in order to reduce the risk of a security breach.

The Fidelis Take

Fidelis Cybersecurity believes that the events detailed in this report are more consistent with cyber criminals than espionage actors. While TTPs analyzed in the recent activity are similar to those employed by espionage actors, they are not unique to them, and there is documented history of shared malware between these two actor sets.[vi] More importantly, we observed that the adversary is saving the document in PPS format in order to bypass all antivirus detection. Furthermore, based on substantial circumstantial evidence, we believe that Nigerian 419 scam actors are involved in at least some of the analyzed activity. This is noteworthy because it would demonstrate these actors' continued evolution of their operations, which has been tracked as early as 2014[vii] and more recently in 2015.[viii] Based on the global scope of the activity detailed in this report, companies should implement the indicators and monitor for similar activity.

There is limited information from which to form an analytic judgment on the individual that built the malware that went undetected by antivirus. At present, there is no reason to suspect that he is involved in conducting any of this activity and we suspect that he is just selling or providing kits to other individuals and groups.

Fidelis Cybersecurity's advanced threat defense product, Fidelis XPS™, detects all of the activity documented in this paper.

For a more detailed look at the technical indicators please see Fidelis Threat Advisory #1017 Appendix

[i] https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4114
[ii] http://www.isightpartners.com/2014/10/cve-2014-4114/
[iii] http://www.washingtonpost.com/r/2010-2019/WashingtonPost/2014/10/14/National-Security/Graphics/briefing2.pdf
[iv] http://krebsonsecurity.com/2015/05/security-firm-redefines-apt-african-phishing-threat/

[v] http://www.pandasecurity.com/mediacenter/src/uploads/2015/05/oil-tanker-en.pdf

[vi] http://www.darkreading.com/analytics/threat-intelligence/cybercrime-cyber-espionage-tactics-converge/d/d-id/1319203

[vii] https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/reports/Unit%2042/419evolution.pdf

[viii] http://www.pandasecurity.com/mediacenter/src/uploads/2015/05/oil-tanker-en.pdf