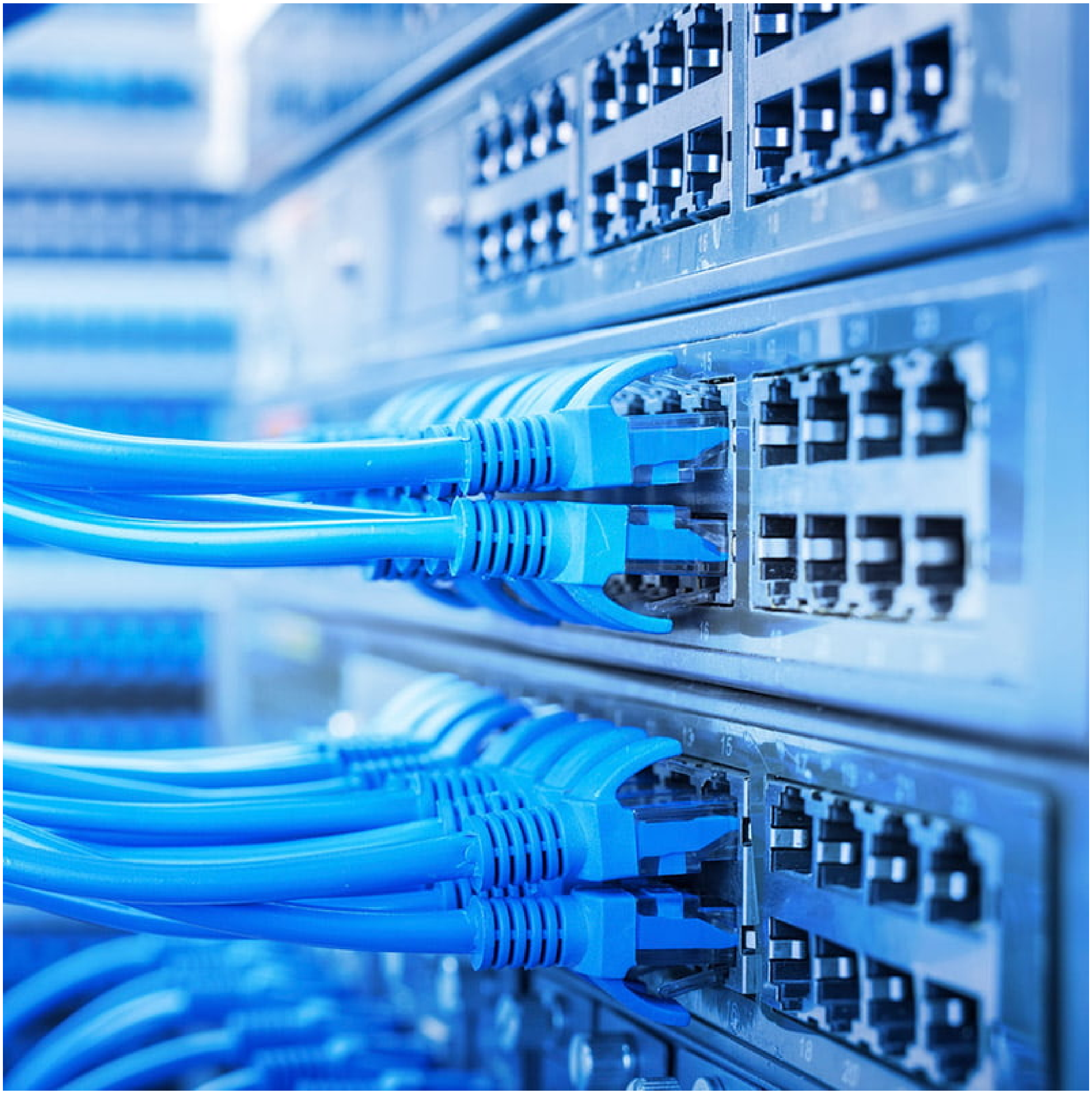
NetWire RAT Steals Payment Card Data

secureworks.com/blog/netwire-rat-steals-payment-card-data

Incident Response Team



Threat actors used a remote access trojan with keylogging capabilities rather than traditional point-of-sale malware Monday, November 28, 2016 *By: Incident Response Team*

During an incident response engagement in September 2016, SecureWorks® incident response analysts observed payment card data being collected by a generic remote access trojan (RAT) rather

than typical memory-scraping malware.

In many payment card data breaches, a point-of-sale (POS) system is infected with malware that searches for specific processes in memory known to store card data in plain text. The malware copies card data from the running processes, a technique known as memory scraping, to encoded files on disk. These files are then transmitted to a threat actor, often over commonly open ports 80 and 443 (HTTP and HTTPS). The threat actor sells the card data or uses it for fraudulent purchases.

In the September 2016 incident, SecureWorks analysts observed card data being collected by the NetWire RAT instead of traditional POS malware. NetWire has a built-in keylogger that can capture inputs from peripheral devices such as USB card readers. The attack methodology is very similar to traditional POS malware. A threat actor sends a phishing email with a malicious attachment to an employee working on a POS computer. If the employee opens the attachment, malware to harvest card data is downloaded or installed. Without proper security protections in place, these infections can remain undetected for months or years.

Keyloggers expose more than just card data; credentials for online accounts and applications such as email, property management systems (PMS), and Internet browsers are at risk. Other sensitive information typed by the user, including Social Security numbers, phone numbers, addresses, and birthdates, can also be compromised. Using a RAT with keylogging capabilities, a threat actor could gather necessary information to commit identify theft and further compromise an organization’s network. The generic NetWire RAT variant used in this incident did not contain specific capabilities to target POS systems.

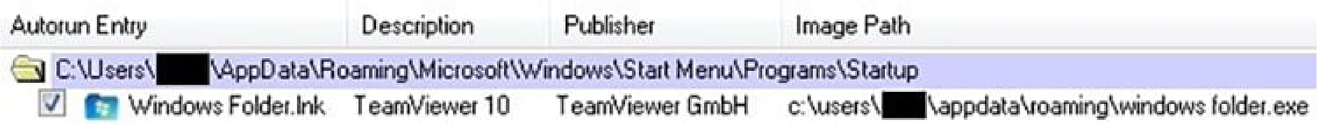
NetWire Details

The NetWire RAT variant observed by SecureWorks analysts has the file description “TeamViewer 10” (see Table 1); however, this binary is not associated with the legitimate TeamViewer application.

Filename	MD5 Hash	Compile Date	File Description	File Version
Windows Folder.exe	378e72e9e4c7ba4ca7498a262c501a54	May 30, 2016	TeamViewer 10	10.0.38475.0

Table 1. NetWire RAT binary details.

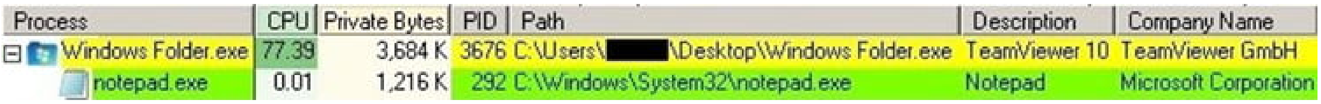
Upon execution, the “Windows Folder.exe” file copies itself to C:\Users\<*username*>\AppData\Roaming and creates a Windows shortcut (LNK) file in the victim’s Startup directory as a persistence mechanism. The Microsoft Autoruns for Windows tool reveals the autostart mechanism that the NetWire RAT creates and uses (see Figure 1). This persistence mechanism ensures that NetWire launches automatically when the victim logs into the system.



Autorun Entry	Description	Publisher	Image Path
C:\Users\[redacted]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup			
☑ Windows Folder.lnk	TeamViewer 10	TeamViewer GmbH	c:\users\[redacted]\appdata\roaming\windows folder.exe

Figure 1. NetWire persistence mechanism. (Source: SecureWorks)

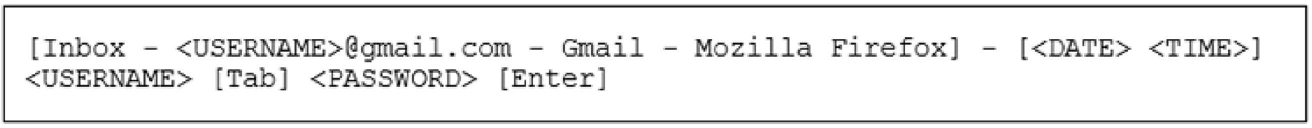
The “Windows Folder.exe” executable spawns and injects code into the legitimate notepad.exe Windows process (see Figure 2). Process injection helps the malware avoid detection; however, review of active network connections show notepad.exe communicating to 185 . 35 . 138 . 227 over port 4588. The notepad.exe process should never have an active network connection.



Process	CPU	Private Bytes	PID	Path	Description	Company Name
⊟ Windows Folder.exe	77.39	3,684 K	3676	C:\Users\[redacted]\Desktop\Windows Folder.exe	TeamViewer 10	TeamViewer GmbH
notepad.exe	0.01	1,216 K	292	C:\Windows\System32\notepad.exe	Notepad	Microsoft Corporation

Figure 2. Child process created by the NetWire RAT. (Source: SecureWorks)

NetWire logs keystrokes and peripheral inputs into encoded files in the C:\Users\<*username*>\AppData\Roaming\Tobe directory. Encoded files observed by SecureWorks analysts have a nomenclature of DD-MM-YYYY. SecureWorks Counter Threat Unit™ (CTU) researchers developed a decoder for these keylogger output files and discovered sensitive information such as track one and track two card data, as well as plain text credentials. The files also display the window title of the opened application, which reveals which application and website the sensitive information was entered. Figure 3 shows an example of a decoded keylogger output.



```
[Inbox - <USERNAME>@gmail.com - Gmail - Mozilla Firefox] - [<DATE> <TIME>]
<USERNAME> [Tab] <PASSWORD> [Enter]
```

Figure 3. Example of decoded keylogger output. (Source: SecureWorks)

Conclusion

Payment card data breaches can cause significant financial and reputational damages for an organization, and can lead to restrictions imposed by compliance bodies and loss of future business. Prevention and detection is critical to ensure that threats to customer data are prevented or detected. Traditional antivirus software and other systems that rely on low-level indicators do not effectively detect and block common and pervasive malware. Organizations should apply endpoint detection mechanisms that apply behavioral analysis and human intelligence to detect threat actor activity.