RESEARCH & INTELLIGENCE

RANSOMWARE USED AS A DISTRACTION

Counter Threat Unit Research Team
February 3, 2016

During a client security intelligence service engagement, SecureWorks Counter Threat Unit™ (CTU) analysts discovered the threat actor using a novel technique to distract responders. By the time the client engaged CTU analysts, the adversary had clearly been established within the compromised infrastructure for some time, had acquired and was actively using the credentials of at least one domain administrator account, and was using those credentials to move throughout the infrastructure via the Terminal Services Client. CTU analysts also observed the threat actor accessing several geographically dispersed domain controllers within a relatively short period of time, indicating that extensive reconnaissance and infrastructure mapping had already occurred.

Through digital forensic analysis of images acquired from several domain controller systems, CTU analysts identified a malicious executable file and supporting VBScript (.vbs) file on one domain controller, as well as an XML file at C:\Windows\SYSVOL\domain\Policies\{31B2F340-016D-11D2-945F-

00C04FB984F9}\USER\Preferences\ScheduledTasks\ScheduledTasks.xml. Partial contents of this XML file are shown in Figure 1.

Figure 1. Partial ScheduledTasks.xml file contents. (Source: Dell SecureWorks)

This file creates a scheduled task that is propagated via Group Policy Objects (GPOs), infecting systems as they join the domain and GPOs are pushed out. The .vbs file referenced within the scheduled task contained code to reach back to the domain controller and then copy and execute the malicious executable file on the local system. As illustrated by the task triggers displayed in Figure 2, the scheduled task was written to persist for only two days.

Figure 2. ScheduledTask.xml trigger. (Source: Dell SecureWorks)

Additional domain controllers contained the same ScheduledTasks.xml and VBScript files that referred back to the malicious executable found on the original domain controller. CTU analysts identified the malicious executable as being associated with ransomware as a service (RaaS). Threat actors can configure these types of executables to encrypt various files found on an infected system. The RaaS provider then takes a portion of the ransom paid by victims as payment.

Placing the malicious executable on one system and the .vbs and .xml files on subsequent domain controllers could have resulted in a devastating mass infection of the infrastructure. If not for a minor misspelling in the ScheduledTasks.xml file, systems across the infrastructure would have been infected during those two days as they joined the domain. This large-scale infection would have presented the IT staff with a significant and potentially overwhelming challenge.

It is likely that the threat actor intended the widespread disruption to distract responders from other malicious activity. The CTU research team recommends that IT administration staff check domain controllers for the existence of ScheduledTasks.xml files and review the content of identified files. These files have legitimate use when knowingly employed within a domain infrastructure, but CTU analysts' observations indicate that they have also been used to attempt mass deployment of malware.

TAGS: Research Blog

ABOUT THE AUTHOR

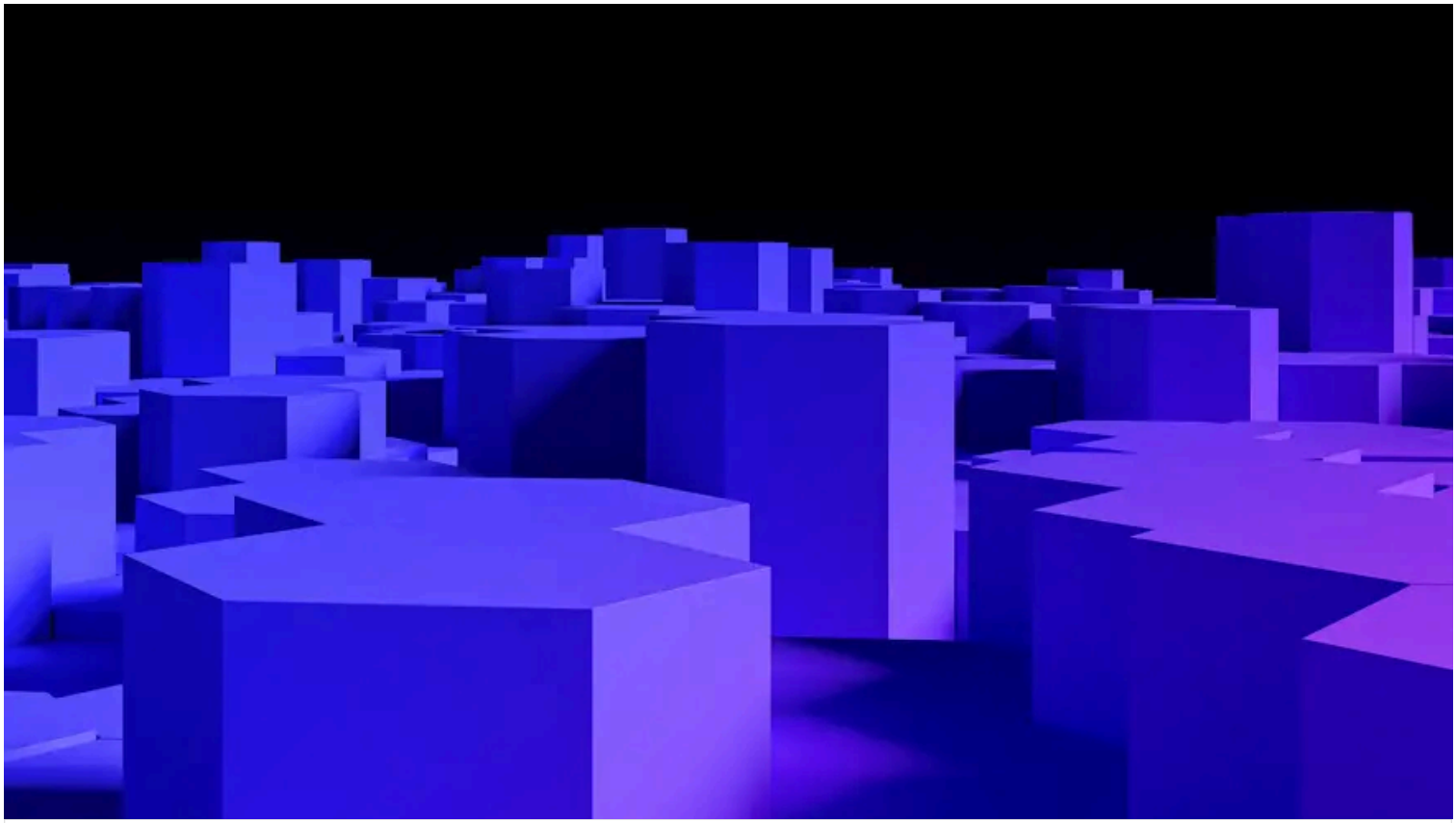
COUNTER THREAT UNIT RESEARCH TEAM

The Secureworks Counter Threat Unit™ (CTU) is a dedicated threat research team that analyzes threat data across our global customer base and actively monitors the threat landscape.

← BACK TO ALL BLOGS

NOW TRENDING...

- 2024 Global State of the Threat Report
- Modernize Your Security Operation Center with XDR
- MDR Done Right



VIRTUAL EVENT

GLOBAL THREAT INTELLIGENCE SUMMIT 2024

WATCH NOW →

GET THE LATEST SECURITY UPDATES

ADDITIONAL RESOURCES

BLOG

THREE CYBERSECURITY PLATFORM PREDICTIONS FOR 2024

READ NOW →

TRY TAEGIS TODAY

Request a demo to see how Taegis can reduce your risk, optimize your existing security investments, and fill your talent gaps.

TRY TAEGIS

Get the latest updates and news from Secureworks.

SUBSCRIBE NOW →

PLATFORM

Detection & Response

XDR

Log Management

MITRE ATT&CK Coverage

Network Security

NDR

Endpoint Security

EDR

NGAV

Identity Security

IDR

OT Security

Operational Technology

Vulnerability Management

Vulnerability Risk Prioritization

WHY SECUREWORKS

Why Secureworks

Customer Trust

Compare Secureworks

At Your Side

ROI Calculator

Artifical Intelligence

Corporate Responsibility

Corporate Overview

Counter Threat Unit

Careers

Investor Relations

SERVICES