illusive™

Cyber Deception Defeats Government Defense Agency's Most Aggressive Attacks

Red Team Case Study

Executive Summary

illusive networks® recently conducted a Capture the Flag exercise for a national defense agency. The agency was evaluating a variety of deception technologies and wanted to investigate forensic data generated by illusive networks solutions during a Red Team exercise.

The exercise was conducted between December 16 and December 20, 2016. Details in this report about the agency's network environment have been obfuscated to protect its privacy.

The agency's representatives knew that deceptions would be deployed. The Red Team environment was set up in a test lab, and they were aggressive in the number and types of attacks they conducted.

illusive's forensic analysis detected malicious activity on three different endpoints in the network. The illusive networks forensic team found evidence of tools and techniques used by the Red Team attacker to collect network intelligence, extract credentials, escalate privileges, and move laterally across the network.

The environment using illusive networks Deceptions Everywhere® technology successfully resisted all of the Red Team's efforts, even though they used a wide variety of sophisticated tools. Government agencies and other organizations with high security needs can use illusive networks to protect their systems against aggressive cyber attackers. Learn why a threat deception approach to cybersecurity, focusing on the humans behind advanced attacks, is the most effective way to deal with modern cyber threats.

How Exactly Does a Cyber "Capture the Flag" Work?

A cyber Capture the Flag exercise is fairly simple — one team takes an offensive role, trying to capture and retrieve a target that is being protected by the defensive team. In this case, the defense agency controlled its network defenses and set them up as they wanted. illusive networks deployed the deceptions and monitored the attacker's progress, analyzing malicious activity and forensic data generated by the deceptions.

The Red Team attacker had multiple success paths available to him and full awareness that illusive deceptions were deployed. If he made a series of correct choices, he would pass through the network undetected on his way to the target. The attacker had access to all attack tools and methods, but illusive networks had the advantage of deception.

Deceptions Everywhere:

A Technical Overview

Cyber attackers are slow and methodical, using various tools and techniques to collect data, analyze it, and move laterally throughout a network. Through trial and error, with enough time, they will find what they are looking for.

Advanced attackers rely on the fact that what they see is real and that the data they collect is reliable. illusive networks Deceptions Everywhere technology combats attackers by introducing an endless stream of false data to the environment. Attackers unknowingly encounter carefully crafted deceptions deployed across the entire network — on endpoints, servers, and attack surfaces — that appear identical to what they need for moving laterally in the network. False data forces attackers to spend more time sifting through what's real and what's illusive, giving the IT team more data and time to make strategic decisions as early as possible in an attack.

illusive installs two new servers on a customer's network — the illusive Deception Management System™ and the illusive Trap Server™. The Deception Management System deploys deceptions across the network that appear real to an attacker. When an attacker accesses a deception on an endpoint, he unknowingly triggers the Trap Server, which interacts with him while running real-time forensics on the source of the attack.

Deceptions are not universal — they are crafted specifically for the organization deploying them and defined using information specific to the company's network. Because the illusive technology is agentless, attackers do not interact with running executables. Deceptions are deployed in such a way that attackers find the deceptions, but the customer's employees do not. By segregating deceptions to the attacker's side, illusive networks virtually eliminates all false positives. High-fidelity alerts enable IT to immediately address an incident knowing that the attack is real.

In the end, illusive networks Deceptions Everywhere technology is built to take the power out of the attacker's hands and return it to the organization's IT and security departments.

"illusive networks Deceptions Everywhere technology combats attackers by introducing an endless stream of false data to the environment."

Deception Strategy: How illusive Approached the Red Team Exercise

The main objective of the forensic analysis was to determine the attacker's goals and deliver actionable evidence and artifacts that help a security team contain an incident. Forensic analysis also enables the defenders to determine which tools the attacker used and how he used them.

Share Deceptions

These deceptions dupe attackers to access fake shared folders and files.

Windows Credentials Deceptions

This information ensnares attackers with non-existent user credentials.

File Deceptions

These deceptions induce attackers to access and use credentials stored in fake files.

Different sets of deceptions are deployed across the assigned computers throughout the network, ensuring that the attacker can't become complacent and rely on consistent data. With the network of deceptions in place, illusive networks was prepared to face the agency's attacker.

> *"Deceptions Everywhere technology tailors deceptions to specifically suit the network being protected."*

Incidents Detected by illusive networks

Forensic data revealed that the attacker appeared to successfully install his complete arsenal of tools, including network enumeration, privilege escalation, and data exfiltration tools. At each machine the attacker reached, he focused first on reconnaissance, attempting to enumerate surrounding machines or existing user credentials. Different deceptions using different techniques were deployed to the lab machines. Multiple deception techniques increased the "fog of deception," making it more difficult for the attacker to avoid triggering an alert.

While he tried to gather information about the network and possible routes to hop through, he unknowingly hit deceptive assets, which triggered alerts in the illusive Deception Management System and initiated collection of forensic evidence.

The illusive forensic application automatically collects attack data in real time from the source of the attack. As the attacker engages with deceptions, illusive networks detects, alerts, and analyzes his movements. illusive's forensic analysts received illusive forensic log files and captures of the traffic between the noted endpoint and the Trap Server. illusive analyzed log files using an in-house automated tool that creates timelines based on the incident timeframes.

When the attacker tried to move laterally across the network, he needed to leverage essential credentials from the involved endpoints. While he scraped passwords and other interesting assets, he also came across deceptive pieces of information. When he tried to use those, the action triggered additional alerts.

The agency's Red Team attacker was highly aggressive, launching a large number of attacks with a comprehensive set of techniques. The techniques he used can be blocked in several ways, because illusive detects lateral movement early and provides data to reveal the attacker's objectives and tools, giving organizations actionable data for mitigation and remediation.

Although the Red Team triggered 11 alerts that delivered valuable forensic data, we only include a portion of those alerts in the event descriptions below.

December 19, 2016

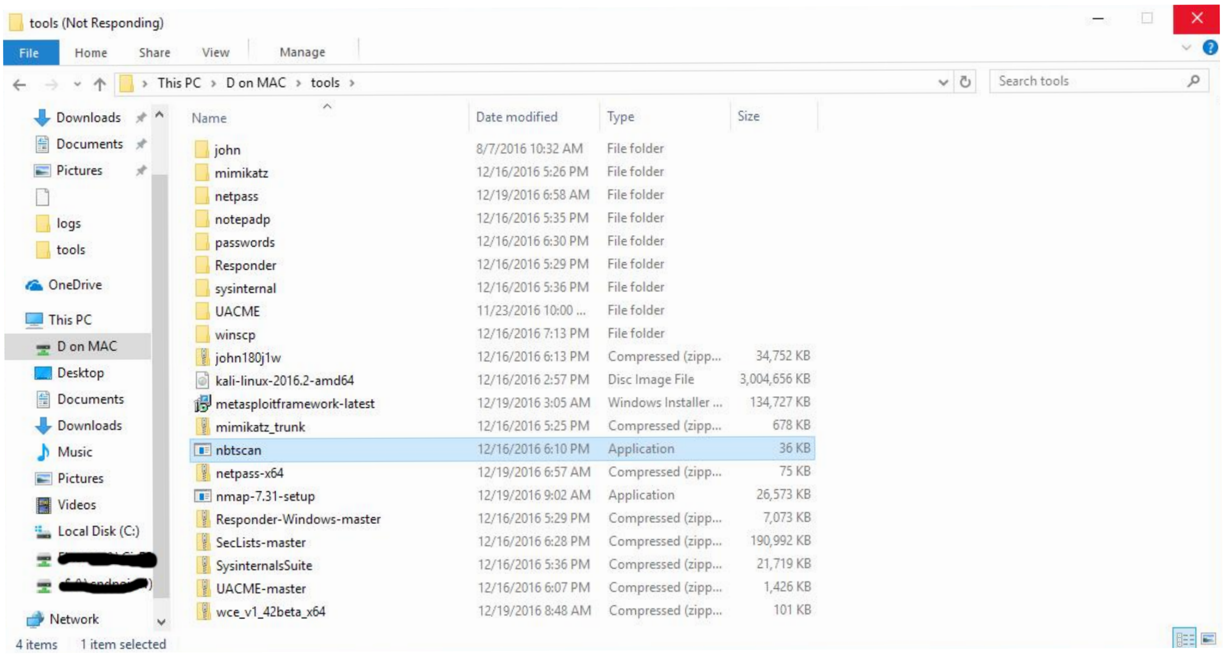
1. illusive first alerted on RDP and scanners incidents that originated from an endpoint named Domaind\Endpoint2. The logged-in user was Domaind\Userj.

2. The attacker found fake RDP credentials and tried to access the deceptive server using the Windows default program (mstsc.exe), first sending ICMP requests (ping) to the Trap server. Once he received a reply, he was tempted to connect to it over RDP.

3. Automatically, illusive collected forensic evidence from the source of the alert. It discovered additional malicious activity performed by the attacker.

4. The attacker accessed his toolset located on his local drive, over rdpclip.exe:

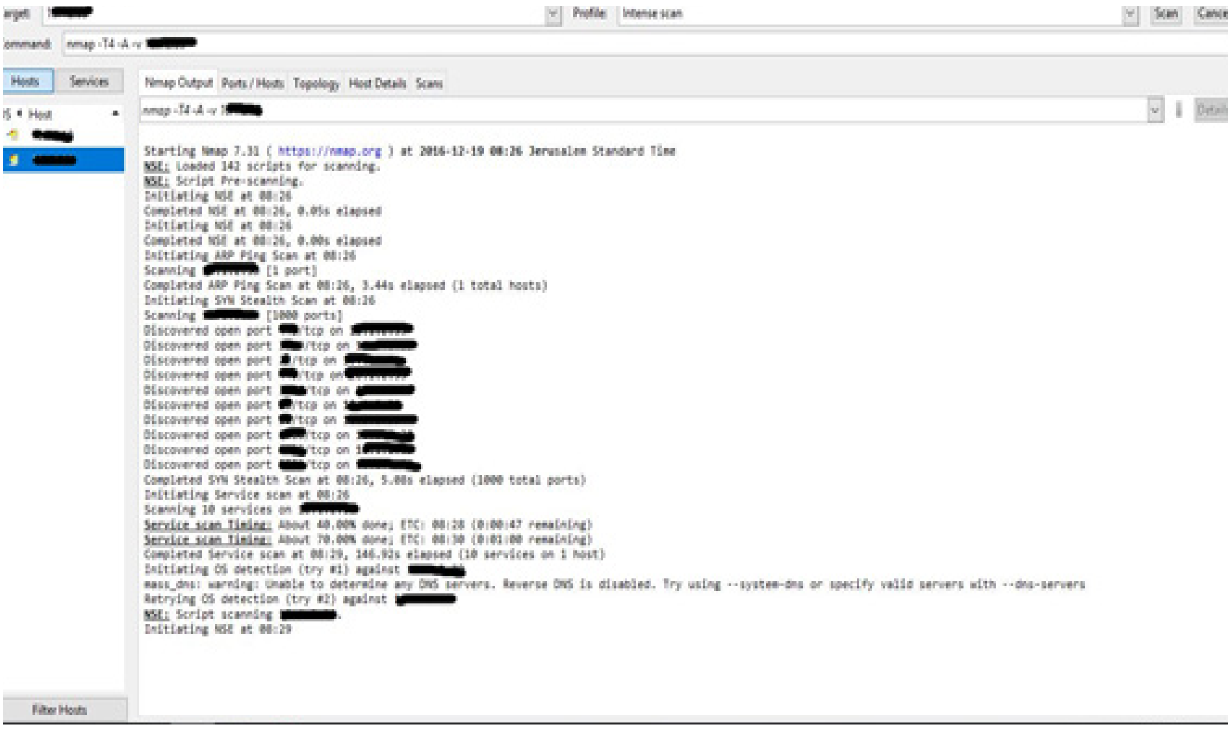
- Mimikatz: used to extract plaintext passwords from memory
- Putty and WinSCP: GUI clients for FTP and SFTP communication
- NetPass: a password recovery utility, used to extract passwords
- Responder and MultiRelay: allows attacker to pivot across compromises
- WCE (Windows Credentials Editor): similar to Mimikatz
- Nmap: network security scanner, used to discover hosts and services
- Nbtscan: a NetBIOS name server scanner



Name	Date modified	Type	Size
john	8/7/2016 10:32 AM	File folder	
mimikatz	12/16/2016 5:26 PM	File folder	
netpass	12/19/2016 6:58 AM	File folder	
notepadp	12/16/2016 5:35 PM	File folder	
passwords	12/16/2016 6:30 PM	File folder	
Responder	12/16/2016 5:29 PM	File folder	
sysinternal	12/16/2016 5:36 PM	File folder	
UACME	11/23/2016 10:00 ...	File folder	
winscp	12/16/2016 7:13 PM	File folder	
john180j1w	12/16/2016 6:13 PM	Compressed (zipp...	34,752 KB
kali-linux-2016.2-amd64	12/16/2016 2:57 PM	Disc Image File	3,004,656 KB
metasploitframework-latest	12/19/2016 3:05 AM	Windows Installer ...	134,727 KB
mimikatz_trunk	12/16/2016 5:25 PM	Compressed (zipp...	678 KB
nbtscan	12/16/2016 6:10 PM	Application	36 KB
netpass-x64	12/19/2016 6:57 AM	Compressed (zipp...	75 KB
nmap-7.31-setup	12/19/2016 9:02 AM	Application	26,573 KB
Responder-Windows-master	12/16/2016 5:29 PM	Compressed (zipp...	7,073 KB
SecLists-master	12/16/2016 6:28 PM	Compressed (zipp...	190,992 KB
SysinternalsSuite	12/16/2016 5:36 PM	Compressed (zipp...	21,719 KB
UACME-master	12/16/2016 6:07 PM	Compressed (zipp...	1,426 KB
wce_v1_42beta_x64	12/19/2016 8:48 AM	Compressed (zipp...	101 KB

5. In addition to the attack tools, the attacker also saved textual files named "passwords.txt" and "mimi_ep5.txt," possibly from output of the above tools.

6. The attacker conducted a scan, which triggered a second alert. Using Zenmap, the GUI version of Nmap, he executed a scan against the assets he found, including the illusive Trap Server.



ommand: nmap -T4 -A -v [redacted]

```
nmap -T4 -A -v [redacted]

Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-19 08:26 Jerusalem Standard Time
NSE: Loaded 142 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:26
Completed NSE at 08:26, 0.05s elapsed
Initiating NSE at 08:26
Completed NSE at 08:26, 0.00s elapsed
Initiating ARP Ping Scan at 08:26
Scanning [redacted] [1 port]
Completed ARP Ping Scan at 08:26, 3.44s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 08:26
Scanning [redacted] [1000 ports]
Discovered open port [redacted]/tcp on [redacted]
Discovered open port [redacted]/tcp on [redacted]
Discovered open port [redacted]/tcp on [redacted]
Discovered open port [redacted]/tcp on [redacted]
Discovered open port [redacted]/tcp on [redacted]
Discovered open port [redacted]/tcp on [redacted]
Discovered open port [redacted]/tcp on [redacted]
Discovered open port [redacted]/tcp on [redacted]
Discovered open port [redacted]/tcp on [redacted]
Discovered open port [redacted]/tcp on [redacted]
Completed SYN Stealth Scan at 08:26, 5.08s elapsed (1000 total ports)
Initiating Service scan at 08:26
Scanning 10 services on [redacted]
Service scan Timing: About 40.00% done; ETC: 08:28 (0:00:47 remaining)
Service scan Timing: About 70.00% done; ETC: 08:30 (0:01:00 remaining)
Completed Service scan at 08:29, 146.92s elapsed (10 services on 1 host)
Initiating OS detection (try #1) against [redacted]
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Retrying OS detection (try #2) against [redacted]
NSE: Script scanning [redacted].
Initiating NSE at 08:29
```

7. After receiving the scan output, the attacker tried to access the Trap Server in multiple ways, including through a deceptive web server via Google Chrome, trying to access a deceptive file server using the default files explorer. By doing so, he triggered an alert.

8. Once the alert was triggered, illusive automatically collected more forensic data, including screen captures of the attacker in action.

Date & Time	Examined Artifact	Findings
19/12/2016 02:45:52	Host Forensics Log	User Domaind\Userj was logged into the first computer (Endpoint2) over RDP
19/12/2016 02:48:51	Host Forensics Log	Mimikatz (plaintexts passwords extraction tool) was first executed on the endpoint
19/12/2016 03:01:13	Host Forensics Log	Using mmc.exe, the attacker exported the local event log into a file and saved it to disk ("ep2")
19/12/2016 05:22:59	Host Forensics Log	WinSCP & Putty GUI clients were copied to the endpoint and executed
19/12/2016 05:59:02	Host Forensics Log	Password recovery utility named NetPass is used to extract clear-text stored credentials
19/12/2016 06:17:10	Traffic Capture Log	ICMP Requests (Pings) are sent from Endpoint2 to the Trap server
19/12/2016 06:18:05	Host Forensics Log	Attacker attempts to open a Remote Desktop Protocol connection to the Trap using mstsc.exe
19/12/2016 06:21:44	Illusive Networks	Additional software is installed and saved under APPS, including PSTools & Python
Console	First Alert – RDP & Scanners Incident	Pythonic web server is installed and set to listen on port 1111: "python -m SimpleHTTPServer 1111"
19/12/2016 06:21:44	Advanced Forensics Log ($MFT)	A toolset to pivot between compromised machines named Responder is moved to the Endpoint
19/12/2016 07:53:15	Advanced Forensics Log (Event Viewer)	Windows Credentials Editor (wce.exe) is installed as a service and executed
19/12/2016 08:05:47	Advanced Forensics Log ($MFT)	Nmap (and its GUI version – Zenmap) is installed on the endpoint and immediately executed
19/12/2016 08:26:30	Host Forensics Log	Attacker uses Zenmap to scan the Trap the service with the command nmap -T4 -A -v -oX x.x.xx
19/12/2016 08:27:08	Illusive Networks Console	Second Alert – Multiple Incidents (Scanners, FTP, SSH, Browsers, Shares & Databases)
19/12/2016 08:43:20	Advanced Forensics Log ($MFT)	A tool used to scan assets based on the NetBIOS protocol, named nbtscan.exe, is copied and executed

December 20, 2016

1. The third alert was an FTP incident. It originated from a different endpoint, Domaind\Endpoint3, where the logged-in user was Domaind\Usert.

2. The attacker encountered a saved connection in the FileZilla client, which pointed him to a deceptive FTP server. Once he attempted to access it, an alert was sent.

3. Once the alert was triggered, illusive automatically collected additional forensic evidence from the endpoint, which revealed more information:

- The attacker first logged on to Endpoint3 with Usert on December 19th
- Some tools also were installed on Endpoint3: Mimikatz and FileZilla

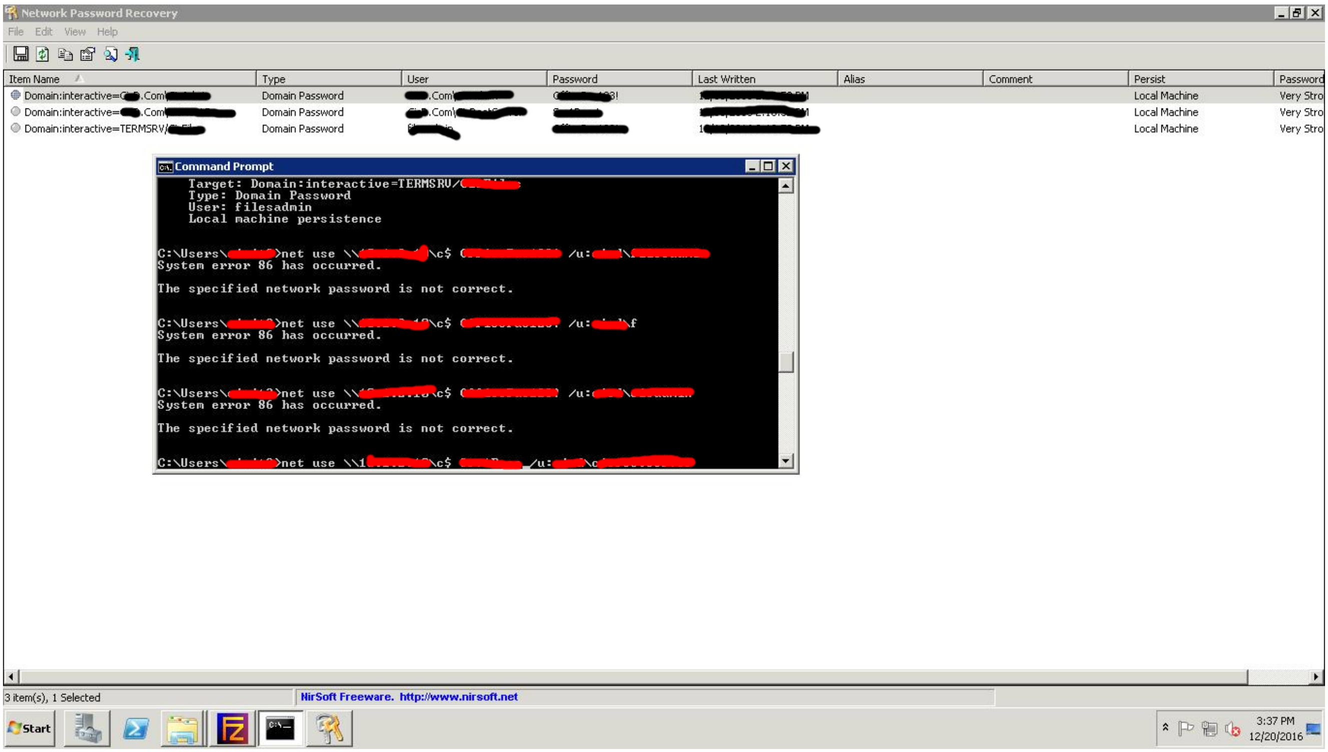
4. The fourth alert was of the Windows family, originating from Endpoint2. The attacker tried to leverage credentials he collected during the previous phase.

5. When he attempted to use deceptive account (Domaind\Endpointw) to authenticate to a server (Domaind\User4), an alert was sent and illusive collected additional artifacts.

6. A fifth Windows alert was sent from a different machine in the environment, a server named Domaind\Server5. The logged-in user was Domaind\Useri.

7. The attacker extracted deceptive credentials from the computer using free software named NetPass and attempted to map the drives on a deceptive server.

8. Using the net use command, the attacker tried to access the Server with multiple deceptive credentials, which triggered more alerts and forensics collection.



Item Name	Type	User	Password	Last Written	Alias	Comment	Persist	Password
Domain:interactive=[redacted].Com\[redacted]	Domain Password	[redacted].Com\[redacted]	[redacted]3!	[redacted]			Local Machine	Very Stro
Domain:interactive=[redacted].Com\[redacted]	Domain Password	[redacted].Com\[redacted]	[redacted]	[redacted]			Local Machine	Very Stro
Domain:interactive=TERMSRV/[redacted]	Domain Password	[redacted]	[redacted]	1[redacted]			Local Machine	Very Stro

```
    Target: Domain:interactive=TERMSRV/[redacted]
    Type: Domain Password
    User: filesadmin
    Local machine persistence


C:\Users\[redacted]>net use \\[redacted]\c$ [redacted] /u:[redacted]\[redacted]
System error 86 has occurred.

The specified network password is not correct.


C:\Users\[redacted]>net use \\[redacted]\c$ [redacted] /u:[redacted]f
System error 86 has occurred.

The specified network password is not correct.


C:\Users\[redacted]>net use \\[redacted]c$ [redacted] /u:[redacted]\[redacted]
System error 86 has occurred.

The specified network password is not correct.


C:\Users\[redacted]>net use \\1[redacted]\c$ [redacted] /u:[redacted]\c[redacted]
```

3 item(s), 1 Selected

NirSoft Freeware. http://www.nirsoft.net

9. The rest of the alerts were Windows alerts, triggered once the attacker tried to authenticate to the DMZ server (Domaind\CisSrvDmz2) using different deceptive credentials.

Date & Time	Examined Artifact	Findings
20/12/2016 01:16:42	Host Forensics Log	On Endpoint2, the attacker accessed files on his computer using notepad, including mimi_ep1.txt file
20/12/2016 01:59:29	Host Forensics Log	Zenmap is executed one more time, however no scan is conducted – possibly for logs restoration
20/12/2016 03:31 - 05:04	Host Forensics Log	Additional hacking tools are installed on Endpoint2 (dirbuster, netcat, metasploit)
20/12/2016 15:28:56	Host Forensics Log	The attacker opened a log file he saved ("mimi_ep1") on his own computer with notepad.exe
20/12/2016 15:29:59	Advanced Forensics Log (Event Viewer)	Attempt to authenticate to a remote server (Server1) with deceptive credentials of Endpointw triggered alert
20/12/2016 15:30:13	Illusive Networks Console	Fourth Alert – Windows Incident
20/12/2016 06:51:48	Host Forensics Log	User Domaind\Useri was logged into the third machine (Server5) over RDP
20/12/2016 15:35:37	Host Forensics Log	The attacker copied again the password recovery tool (NetPass) in order to extract credentials
20/12/2016 15:36:31	Host Forensics Log	Using net use command, the attacker tried to map remote drives on deceptive severs and triggered alert
20/12/2016 15:36:59	Illusive Networks Console	Fifth Alert – Windows Incident

What Can illusive networks Deceptions Everywhere Technology Do for You?

Prevention technologies are not enough to protect an organization. Cyber attackers are relentless, continuing to customize their attacks until they find a way to penetrate the network. They don't stop until they find what they're looking for—whether it's a credit-card database, file server with client information, or other sensitive assets.

These attacks are called Advanced Persistent Threats (APT), and they are expected to continue increasing, targeting a growing number of industries. APT attacks pose serious financial threats to their targets, as well as fundamental threats to their brands. Deceptions Everywhere technology weaves a deceptive layer over the entire network, creating an environment where attackers cannot rely on the information they collect. If attackers can't collect reliable data, they can't make decisions. And if they can't make decisions, the attack is paralyzed.

- **Agentless Deployment** illusive networks improves the organization's security posture without placing costly, complicated management applications on endpoints. Because the entire network is covered with deceptions, illusive creates an endless maze of false data. An attacker can't distinguish between real and fake information, slowing progress toward critical assets.

- **Unprecedented High Detection** illusive detects lateral movements after the attacker has penetrated your defenses. With every endpoint, server, and component coated with illusive deceptions, attackers cannot avoid detection. Using advanced machine learning, illusive automatically creates, instantly diversifies, and optimally deploys deceptions based on your corporate environment conventions. This enables illusive to disrupt and detect breaches without interrupting business.

- **An Attacker's Perspective** Expose attackers by turning their strengths into weaknesses. illusive Attacker View™ puts you inside the mind of an attacker, allowing you to view your entire network from the attacker's perspective. Now you can map your network to more easily analyze, assess, and minimize potential attack risks.

- **Actionable Detection for Greater Security** illusive provides concrete evidence of a breach, containing all supporting forensics — in real time — from the source of the attack. Comprehensive forensics unveil attack location, path, techniques, and context to enable efficient incident response.

The government agency's Red Team learned first-hand the power of illusive networks innovation. Even with a wide range of tools, privilege escalation capabilities, and knowledge of the network, the team's efforts were completely exposed. They failed to capture the flag. Your organization's network can be protected like this, too.

Learn how illusive networks can keep your network safe.

By creating a deceptive layer across the entire network – agentlessly deployed on every endpoint, server and network – illusive networks disrupts and detects breaches with source-based, real-time forensics without interrupting business. Visit www.illusivenetworks.com. Follow us on Facebook and Twitter @illusivenw.

Follow us @illusivenw and on Facebook www.facebook.com/illusivenetworks/