Behind Closed Doors: The Rise of Hidden Malicious Remote Access

By Cybereason Security Services Team

Archived: 2026-04-05 23:00:22 UTC

Cybereason Security Services issues Threat Analysis reports to inform on impacting threats. The Threat Analysis reports investigate these threats and provide practical recommendations for protecting against them.

In this Threat Analysis Report, Cybereason's Security Research Team explores the security implications, vulnerabilities, and potential mitigation strategies surrounding Hidden VNC (hVNC) and Hidden RDP (hRDP), as well as showcasing examples of current usage by malware authors to shed light on the evolving landscape of virtualized infrastructure security.

KEY OBSERVATIONS

- **Stealthy Operations:** hVNC and hRDP allow attackers to maintain persistent, undetected access to systems under their control by creating invisible desktop sessions or modifying RDP services, challenging traditional detection methods.
- **Sophistication and Resourcefulness:** Employed by advanced threat actors, these techniques demonstrate a high level of sophistication, leveraging legitimate system functionalities for malicious purposes, thus complicating the differentiation between benign and malicious activities.
- **Versatile Malicious Use:** Beyond persistence, hVNC and hRDP are utilized for data exfiltration, deploying additional malware, and facilitating ransomware attacks, showcasing their versatility in cybercriminal operations.
- **Detection and Mitigation Challenges:** The covert nature of these techniques eludes standard security defenses, necessitating advanced solutions like behavioral analytics and endpoint detection and response (EDR) systems capable of identifying anomalous activities associated with hidden sessions.
- **Accessibility in the Cybercrime Ecosystem:** The availability of hVNC and hRDP capabilities on dark web marketplaces indicates a demand among cybercriminals, lowering the entry barrier for attackers without the technical expertise to develop these methods independently.

What Is hVNC?

Foundations of Remote Access - VNC

Virtual Network Computing (VNC) is a protocol that facilitates remote desktop sharing and control, essentially allowing users to interact with distant computers as if they were sitting in front of them.

It operates on a server/client model where the VNC server runs on the computer being accessed remotely, and the VNC client, or viewer, runs on the computer from which the user wants to control the remote machine.

Leveraging the Remote FrameBuffer (RFB) protocol, VNC transmits the keyboard and mouse inputs from the client to the server, while the server sends back the graphical screen updates, enabling real-time remote interaction.

This technology supports a wide range of applications including remote administration, providing technical support, and enabling collaborative work, thus empowering users with flexibility and immediate access to information and software on remote systems.

The Stealthy World of hVNC

Amidst the legitimate applications of VNC, however, lies its clandestine counterpart – hidden VNC (hVNC). This technique, exploited by cybercriminals, deploys malicious software embedded with a VNC server component, providing them with covert access and control over an infected system,

The "hidden" aspect of hVNC refers to its ability to operate undetected, making it an formidable tool in the hands of malicious actors. The covert functionality it delivers paves the way for a wide array of nefarious activities, from unauthorized system access to the theft of sensitive data, significantly elevating the level of threat to the targeted system.

Under the Hood of hVNC

Exploring the mechanics of hVNC reveals that it utilizes the Microsoft Windows Desktop API to craft a hidden desktop via the Windows feature CreateDesktop.

This concealed desktop remains invisible to users, complicating the challenge of uncovering its presence. Moreover, hVNC capabilities go beyond mere observation, actively emulating keyboard and mouse input, allowing cybercriminals to navigate compromised systems with precision.

Yet, employment of hVNC is far from trivial; it represents a step up in sophistication and technical acumen by malware authors. The technology's utilization requires not only an in-depth understanding of Microsoft Windows' core functionality but also the ability to manipulate those features for malicious purposes.

```
}
[DllImport("user32.dll", SetLastError = true)]
private static extern IntPtr OpenDesktop(string lpszDesktop, int dwFlags, bool fInherit, uint dwDesiredAccess);

[DllImport("user32.dll", SetLastError = true, CharSet = CharSet.Unicode)]
private static extern IntPtr CreateDesktop(string lpszDesktop, IntPtr lpszDevice,
    IntPtr pDevmode, int dwFlags, uint dwDesiredAccess, IntPtr lpsa);
```

Example Of Win32 API Calls Included In Various RATs

For instance, adapting hVNC to support multiple desktops and replicate user inputs reflects a complex challenge due to VNC's inherent limitations in supporting multiple desktop environments.

Microsoft's documentation notes that creating additional window stations and desktops is feasible via the CreateWindowStation and CreateDesktop functions. However, the ability to create these environments is bounded

by the system's desktop heap capacity, pointing to the intricate nature of hVNC's deployment in circumventing traditional remote desktop capabilities.

What is hRDP | RDP Overview

Remote Desktop Protocol (RDP), developed by Microsoft, enables users to remotely access and control a computer across a network, offering a way to interact with a distant system's desktop environment directly. Similar to Virtual Network Computing (VNC), RDP allows for full graphical control of a remote machine, facilitating tasks such as remote administration, technical support, and access to resources as if directly interacting with remote system.

RDP Connection Prompt

Both protocols serve the essential function of bridging distances between users and systems, ensuring that interactions are as intuitive and productive as if they were performed locally. While VNC is platform independent, RDP, with its proprietary design, specifically caters to Windows environments, providing a seamless and integrated experience that supports a wide range of applications and tasks across remote connections.

hRDP

Hidden Remote Desktop Protocol (hRDP) represents an illicit adaptation of Microsoft's RDP, engineered for covert remote access and control over a compromised computer. Distinct from legitimate RDP use, hRDP facilitates hidden operations, thereby enabling attackers to manipulate a victim's PC invisibly.

The technique typically involves manipulating Windows session management and desktop display settings, allowing hRDP sessions to run without displaying any activity on the compromised machine's monitor. Attackers usually accomplish this by reconfiguring the RDP service to listen on a non-standard port and establishing secret user accounts for surreptitious access. Consequently, attackers can perform operations as if they were directly interacting with the system, such as running commands, installing unauthorized software, or extracting data, all without alerting the user or being flagged by security systems.

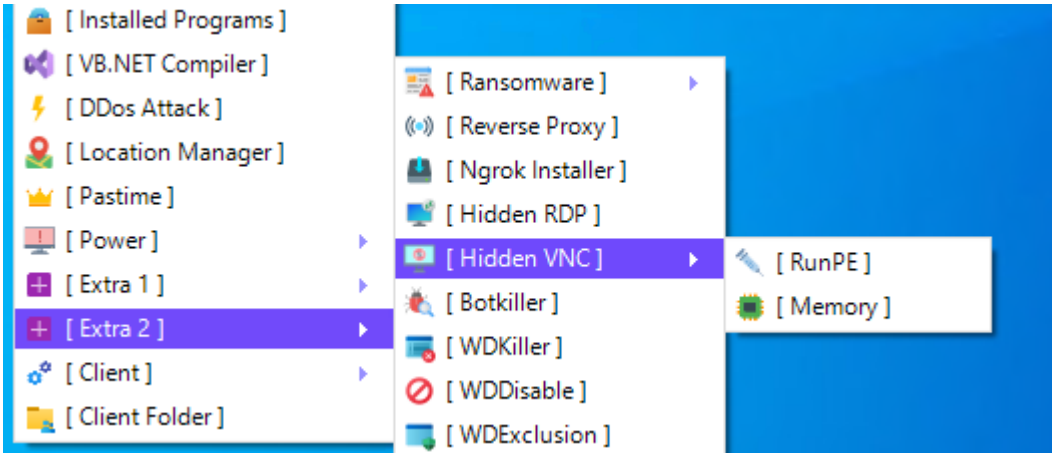
Malware often paves the way for hRDP by installing the components needed for its operation, effectively transforming the infected machine into a controlled node for surveillance, command execution, and the dissemination of further malicious payloads. The covert operation of hRDP makes it an insidious method for persisting stealthily on networks, facilitating espionage, data exfiltration, and serving as a foothold for broader attacks within the victim's environment.

ANALYSIS

This section covers an overview of different Remote Access Tools (RAT) implementing hidden VNC/RDP capabilities as discovered across multiple malware forums.

RATs (Remote Access Trojans) are a type of malware designed to provide an attacker with control over a victim's computer remotely. A RAT typically infiltrates a system through phishing emails, malicious downloads, or vulnerabilities in software.

In most contemporary RATs, malware authors are increasingly integrating hVNC and hRDP as optional features. These techniques are, of course, favored by criminal actors for their effectiveness in maintaining persistent, stealth access to compromised systems.



XWorm User Interface Showing Inclusion Of hVNC & hRDP Features

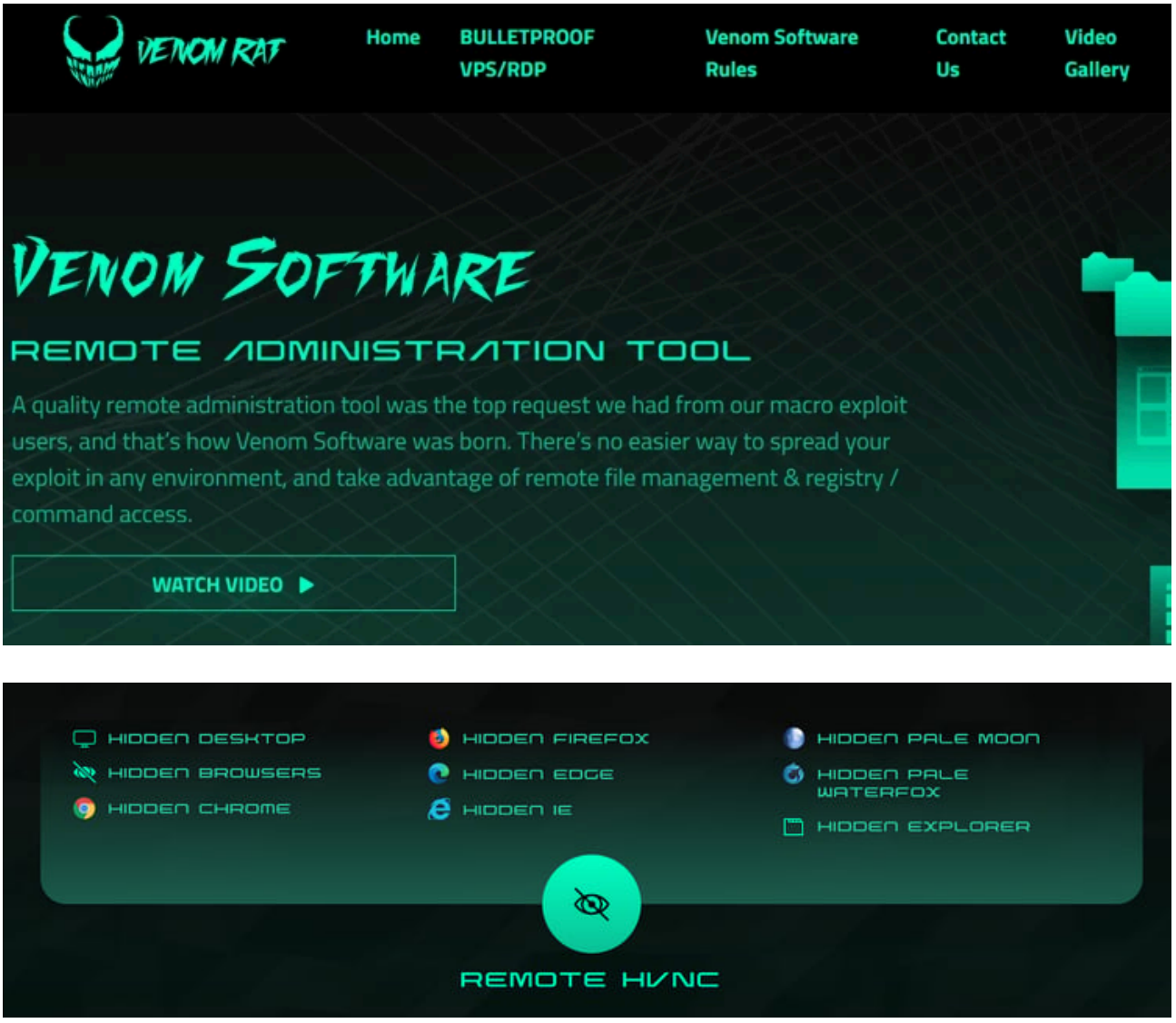
RAT Advertising In Malicious Forums

Malware forums and dedicated Malware-as-a-Service (MaaS) websites represent the evolution of the landscape of cybercrime and the commercialization of malware tools. These platforms not only provide a marketplace but also act as a hub for the exchange of knowledge and tactics among cybercriminals. Among the wares advertised, RATs with hVNC or hRDP are becoming more common.

Cybereason Security Research uncovered various websites promoting such malware and their hRDP/hVNC features.

Venom RAT

A successor to Quasar RAT known for its wide array of malicious capabilities, Venom RAT is a multi-function malware tool that supports keylogging, surveillance, file management, and remote command execution. Use of hVNC to remain hidden on infected machines is offered as a premium feature for purchase, and includes customer support.

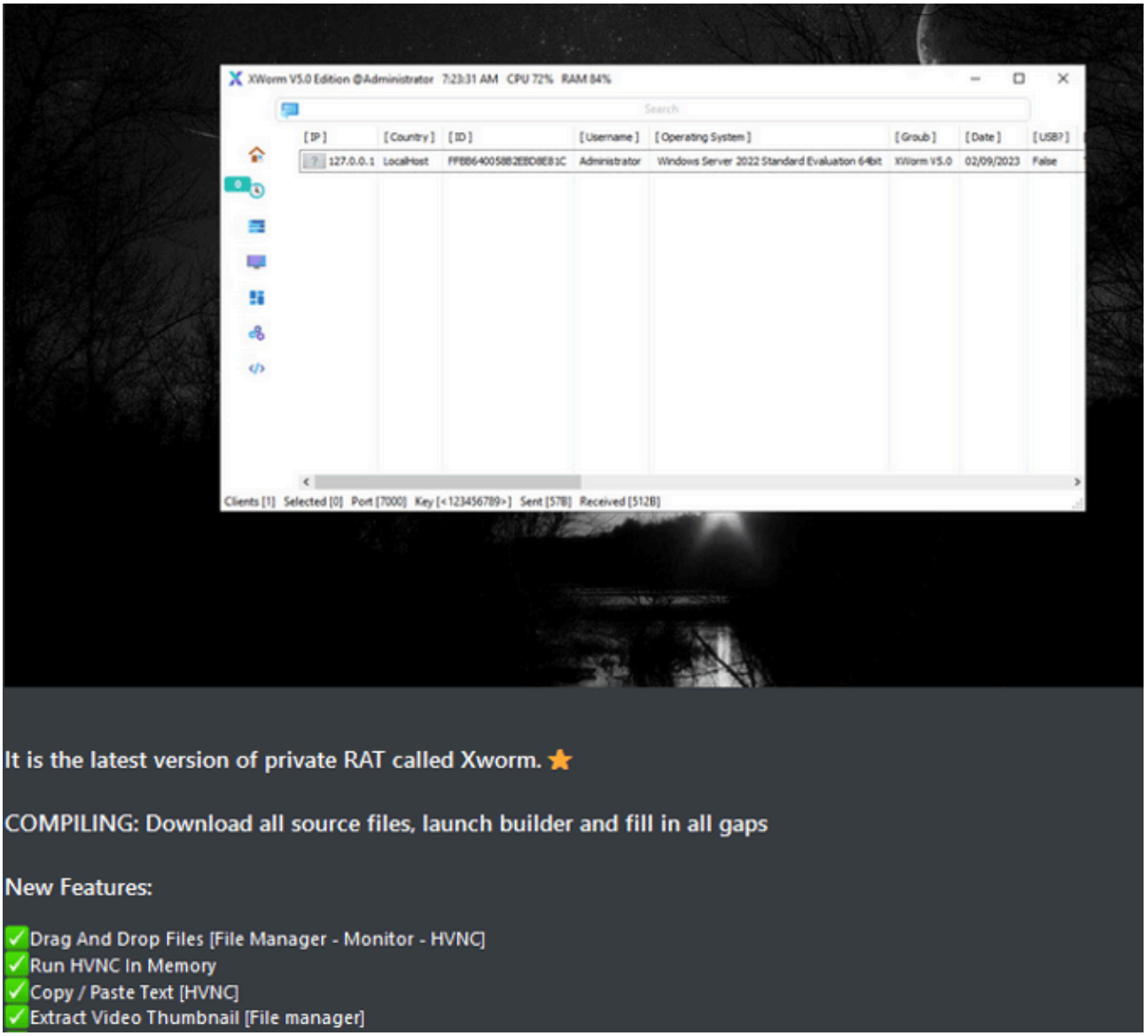


Example Of Venom RAT With hVNC Feature On Dedicated Website

XWorm RAT

XWorm RAT is another tool that has gained attention for its robust functionality and flexibility. With features designed for espionage, data theft, and system manipulation, XWorm RAT provides attackers with a comprehensive toolkit for targeting Windows operating systems.

Its encryption of communications between the client and server ensures that transactions remain secure and hidden from network monitoring tools. It now includes advanced hVNC features like copy/paste and file management and monitoring, enhancing the attacker's control over the compromised system. XWorm's capability to run hVNC directly in memory further obscures its presence.

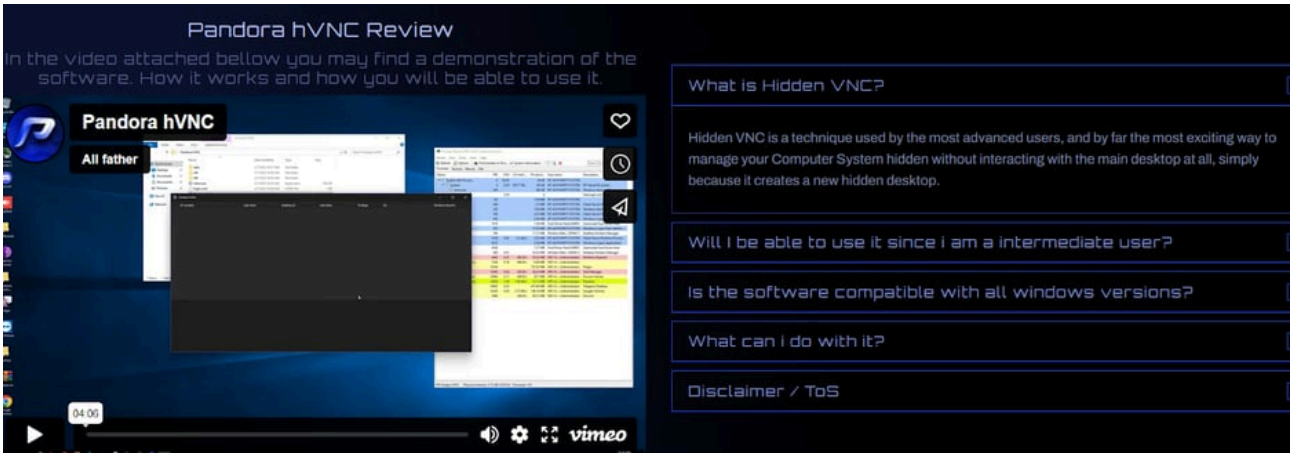


Example Of XWorm RAT With hVNC & hRDP Features Offered On Malware Forums

Pandora hVNC

Pandora hVNC is a RAT that has been circulating in cybercrime forums since 2021 with an established reputation as a preferred tool among threat actors for covert system control. Similar to Venom RAT, it is marketed under the guise of a legitimate remote access software. However, Pandora hVNC features betray its malicious intent.

It employs reverse connection techniques to circumvent firewall restrictions and includes a lightweight TCP server for efficient and encrypted remote command and control operations. This tool enables complete access and control over infected systems, including mouse and keyboard inputs, and can even navigate two-factor authentication in certain scenarios. Additional features include browser profile cloning for data theft, process suspension, CMD/PowerShell access, crypter compatibility for code obfuscation, and stealth operations through memory-only stub injection, all contributing to its evasion of antivirus detection.

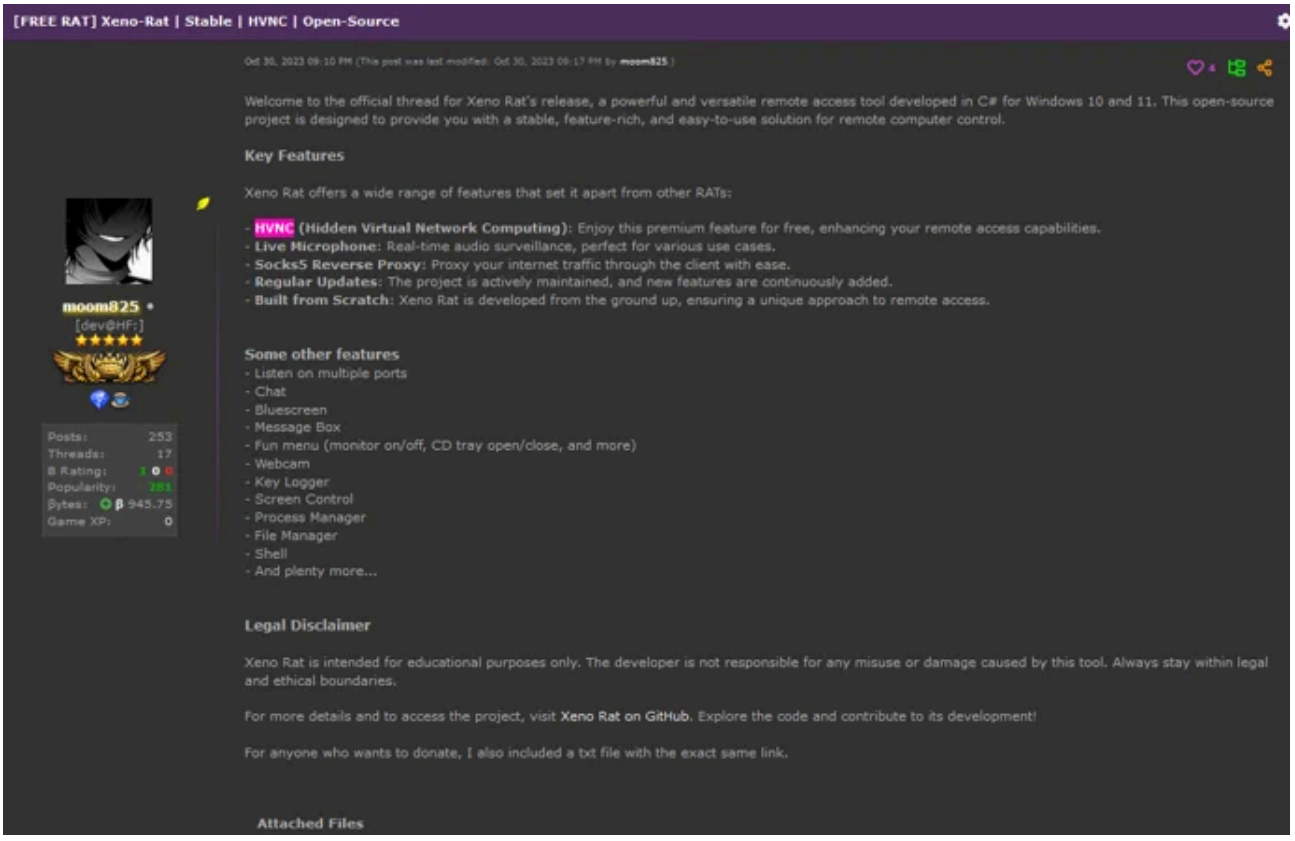


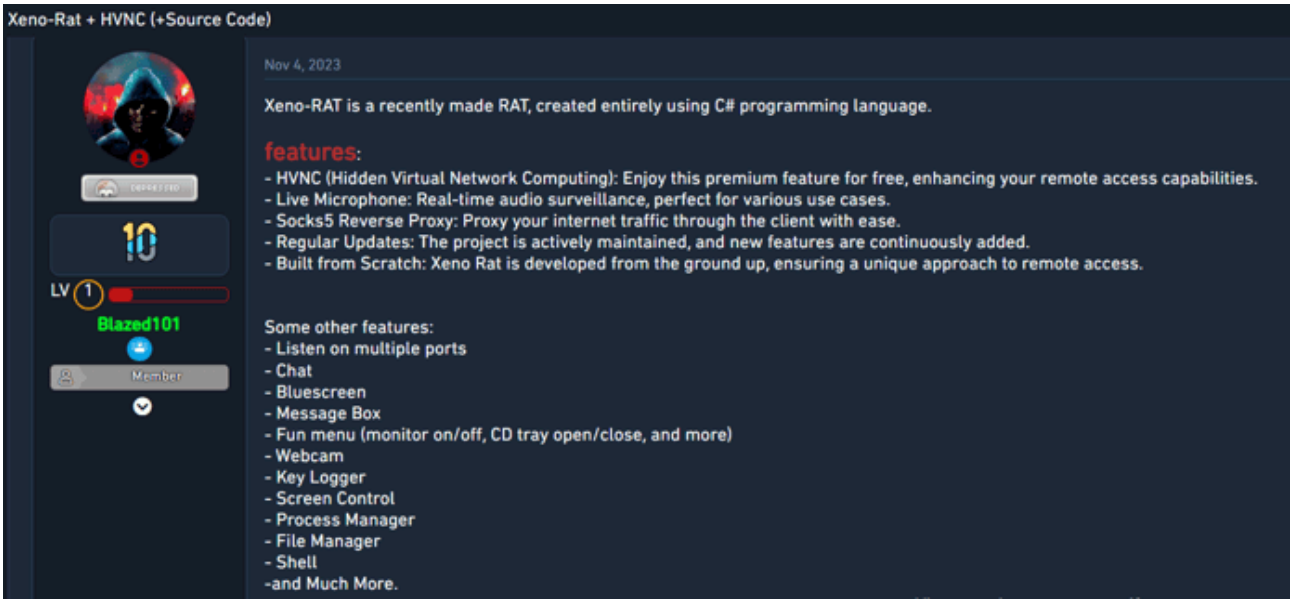
Example Of Pandora hVNC Feature In The Dedicated Website

Xeno RAT

Xeno RAT, designed for Windows operating systems, is notable for its integration of hVNC. Written in C# and advertised as open-source, Xeno RAT distinguishes itself by providing hHVNC as a standard feature—uncommon in other RATs where it might be a premium addition. This allows for undetected remote desktop access, enabling attackers to execute actions on the victim's computer without their knowledge.

Alongside hVNC, Xeno RAT boasts a comprehensive feature set aimed at surveillance and system manipulation, including live microphone access, a Socks5 reverse proxy for bypassing network restrictions, and regular updates enhancing its effectiveness and user experience. Its development from scratch signifies a tailored approach to remote access, emphasizing ease of use without compromising on power or versatility



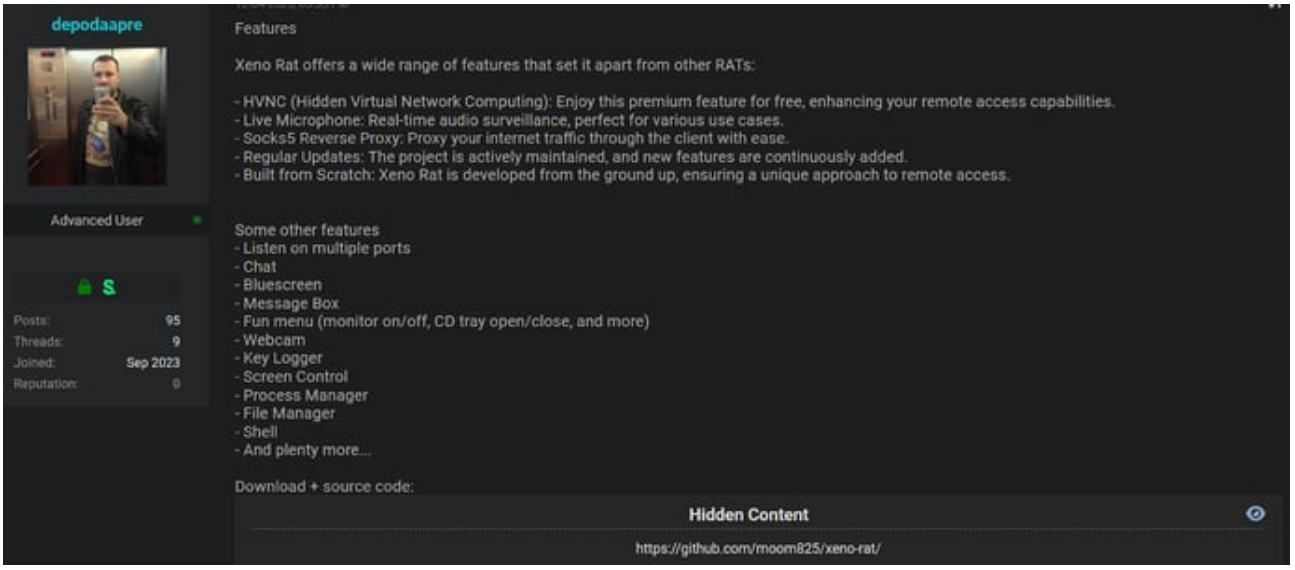


Examples Of Xeno RAT With hVNC & hRDP Features

Prolific Marketplace

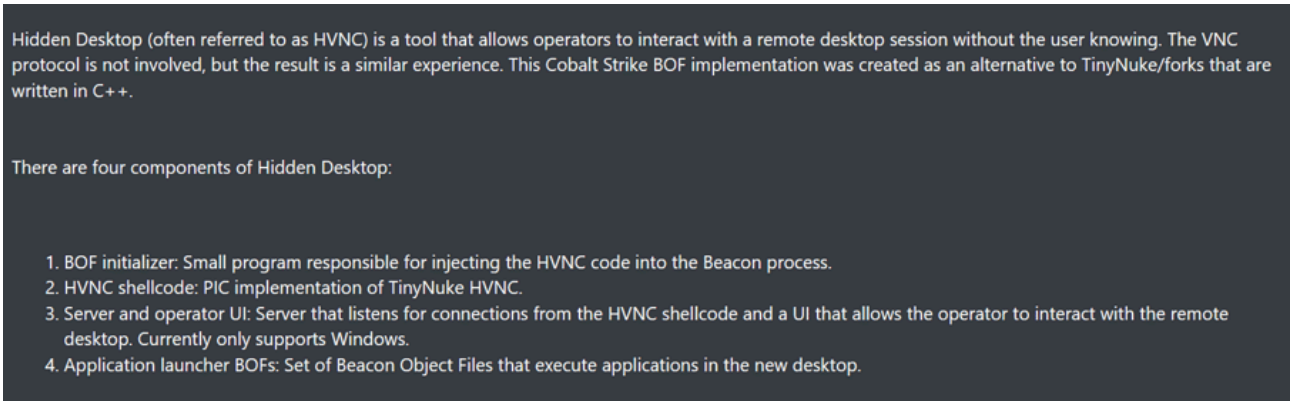
The cybercrime ecosystem thrives via malware forums and dark web marketplaces acting as hubs for the trade of advanced tools and services. Screen captures from these forums reveal listings for malware like hRDP-enhanced tools and Xeno RAT, illustrating the widespread availability and demand for such capabilities.

Example Of Selling hRDP Access On Malware Forums



Malware Seller Account On Malware Forums

The Cybereason Security Research Team was even able to discover a Cobalt Strike Beacon Object File (BOF) implementation of a Hidden Desktop, signaling a continuous innovation and lowering the barrier for entry to what's possible in remote system manipulation and monitoring.



Cobalt Strike BOF Offering Hidden Desktop Features

As these platforms continue to facilitate the proliferation of advanced malware tools, the digital battleground becomes increasingly complex, with hVNC and hRDP serving as critical components in the ever-expanding toolkit of the modern cybercriminal.

hVNC and hRDP Features Behavioral Analysis

In this chapter, the Cybereason research team detonated Xeno RAT and XWorm RAT and observed the resulting behaviors of using the hVNC and hRDP modules of the malwares. This analysis helps building new detections and understanding how these functionality work at operating-system level.

Xeno RAT Analysis (hVNC feature)

When Xeno RAT is deployed on the victim host, as indicated in the screenshot below, we can observe that Google Chrome opened on the attacker machine via hVNC is not visible on the victim machine.

Powershell commands executed via hVNC from the attacker's machine also remain invisible to the victim.

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --no-sandbox --allow-no-sandbox-job
--disable-gpu --user-data-dir=C:\ChromeAutomationData
```

Command Line Used By RAT To Open Chrome Via hVNC

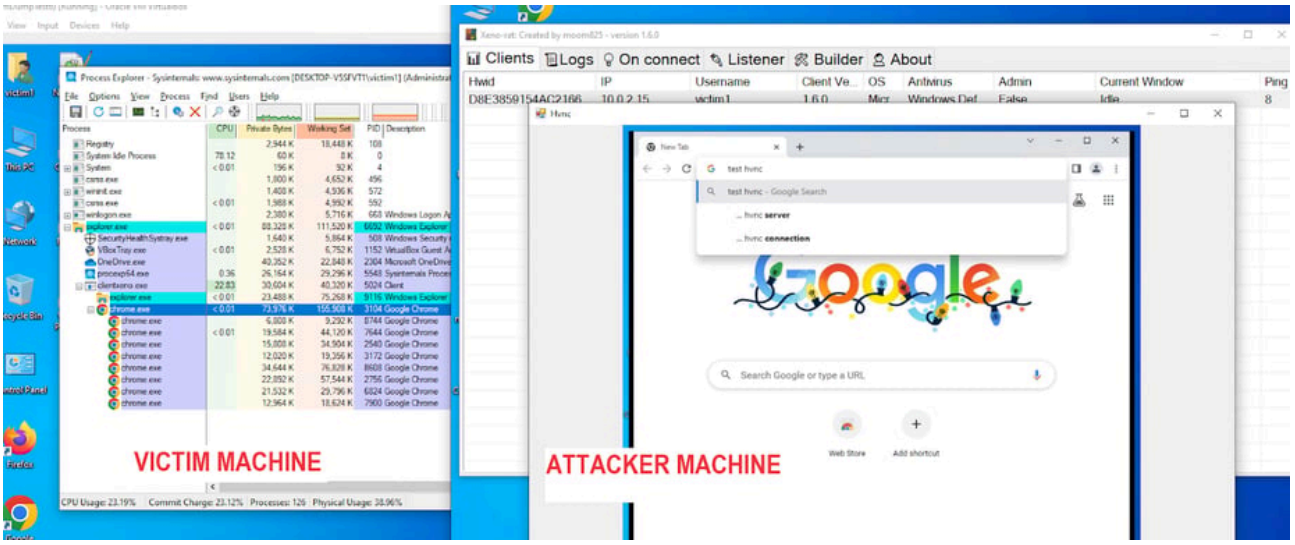
In the Xeno RAT lab tests, *Process Explorer* identified two *explorer.exe* processes on the victim's machine. One was attributed to the attacker, concealed from the victim's desktop but visible on the attacker's hVNC desktop.

Crucially, hVNC is compatible with major browsers, applications, and tools. In this case, Chrome and PowerShell operate as child processes to the attacker-controlled *explorer.exe.*

XWorm RAT Analysis

hVNC Feature (XWorm)

Similar to our previous testing but using XWorm RAT, we simulated an attacker opening a browser window covertly on the compromised system.

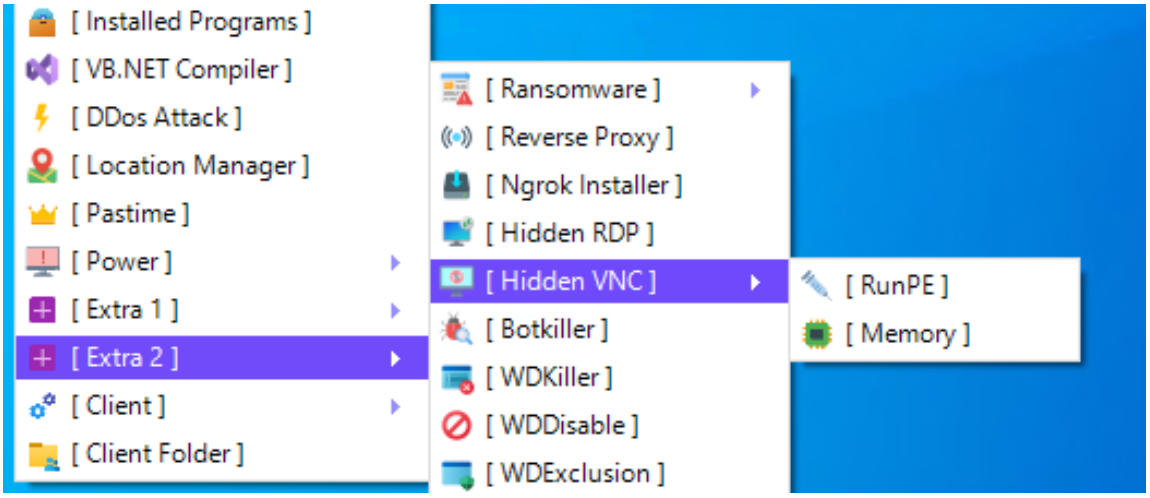


Command Line Used By RAT To Open Chrome Via hVNC

In the XWorm graphical user interface, attackers have the option of deploying hVNC either in RunPE or in memory. RunPE involves executing the hVNC process by injecting it into a legitimate running process executable

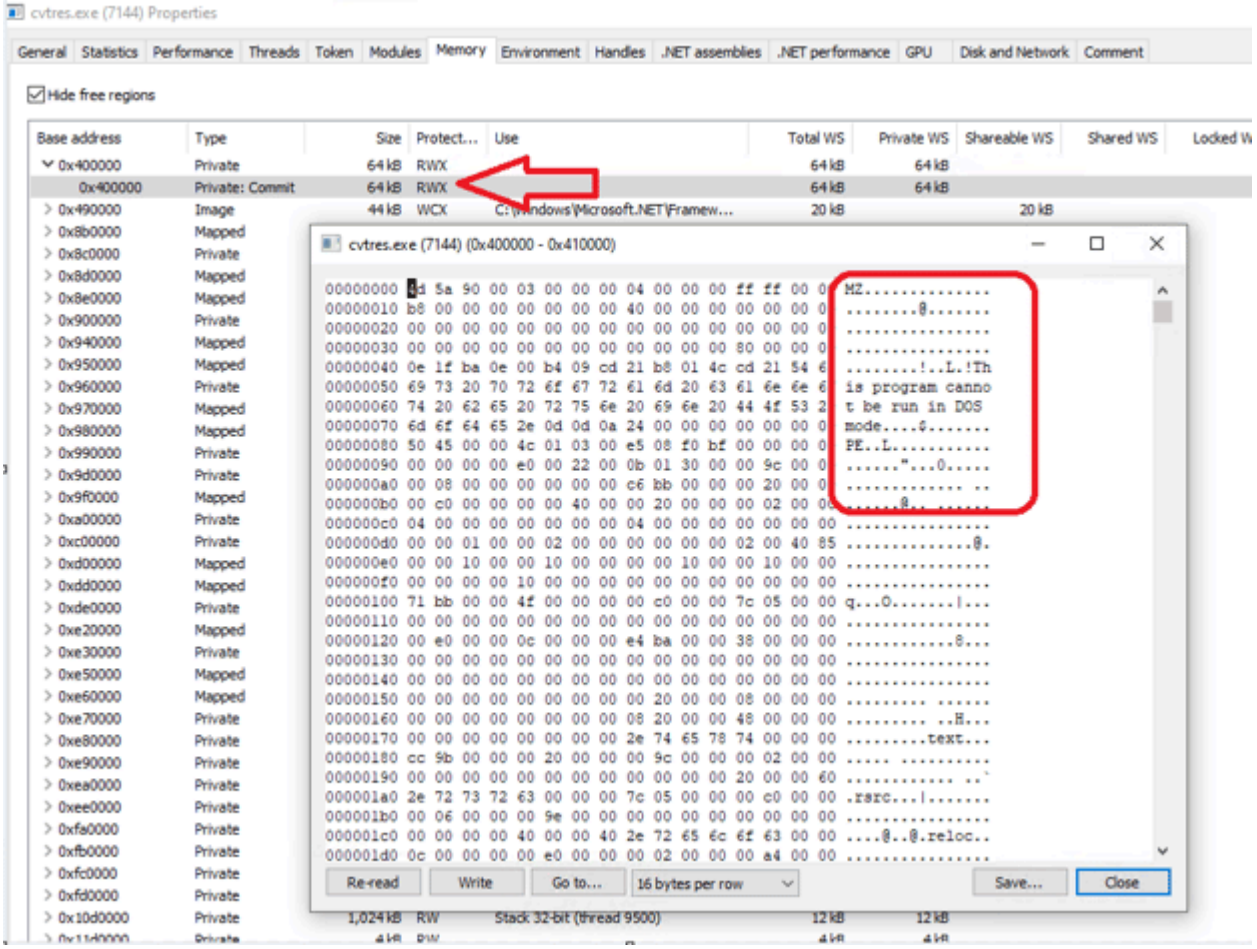
(PE) on the disk, which can potentially leave traces or artifacts that might be detected by security solutions.

The alternative refers to running the hVNC process entirely in the system's RAM without writing any part of it to the disk, making it more stealthy and harder for antivirus programs to detect.



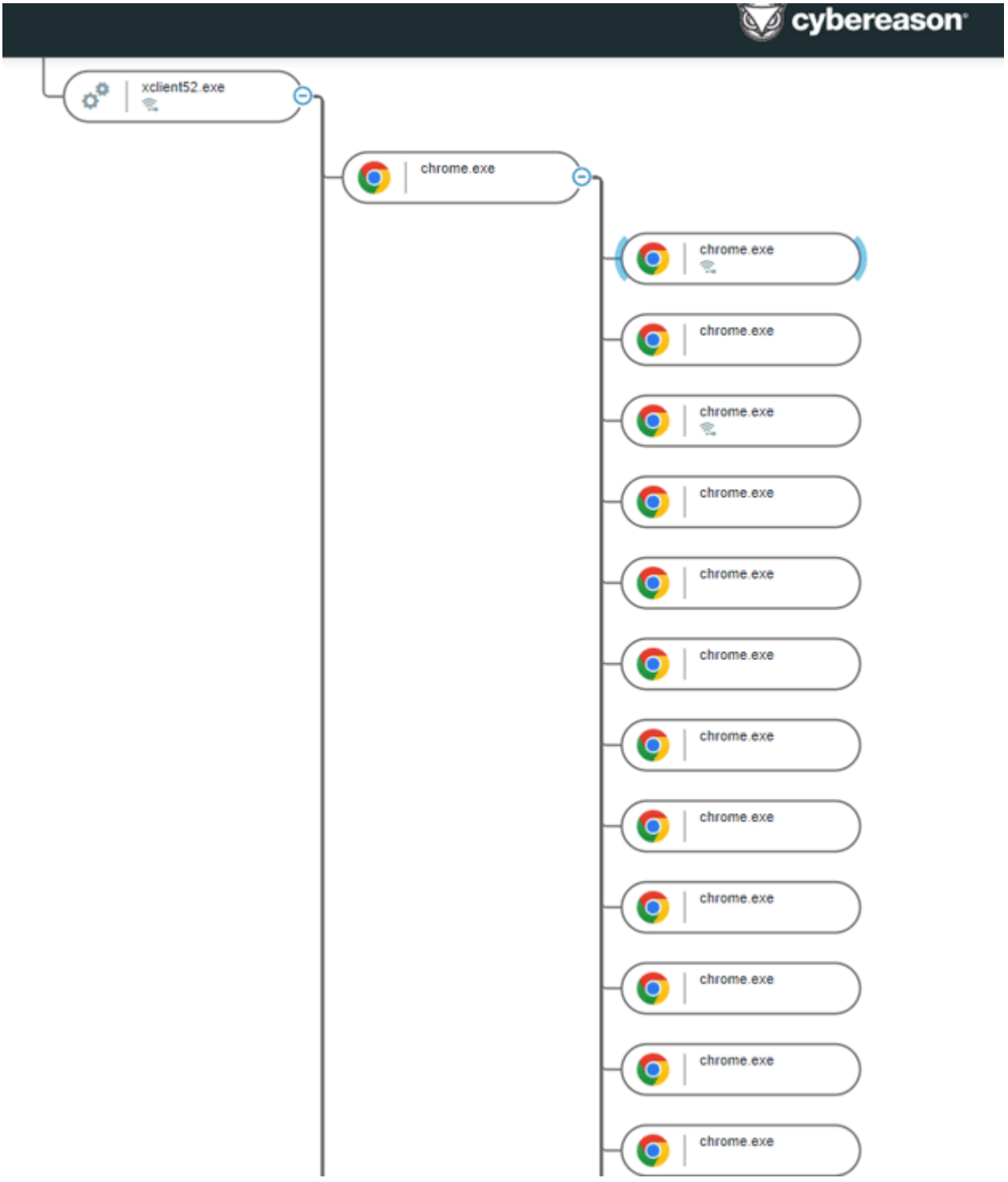
XWorm hVNC Menu Options

In this example, we identified that the attack leverages the legitimate process *cvtres.exe* to inject its code.



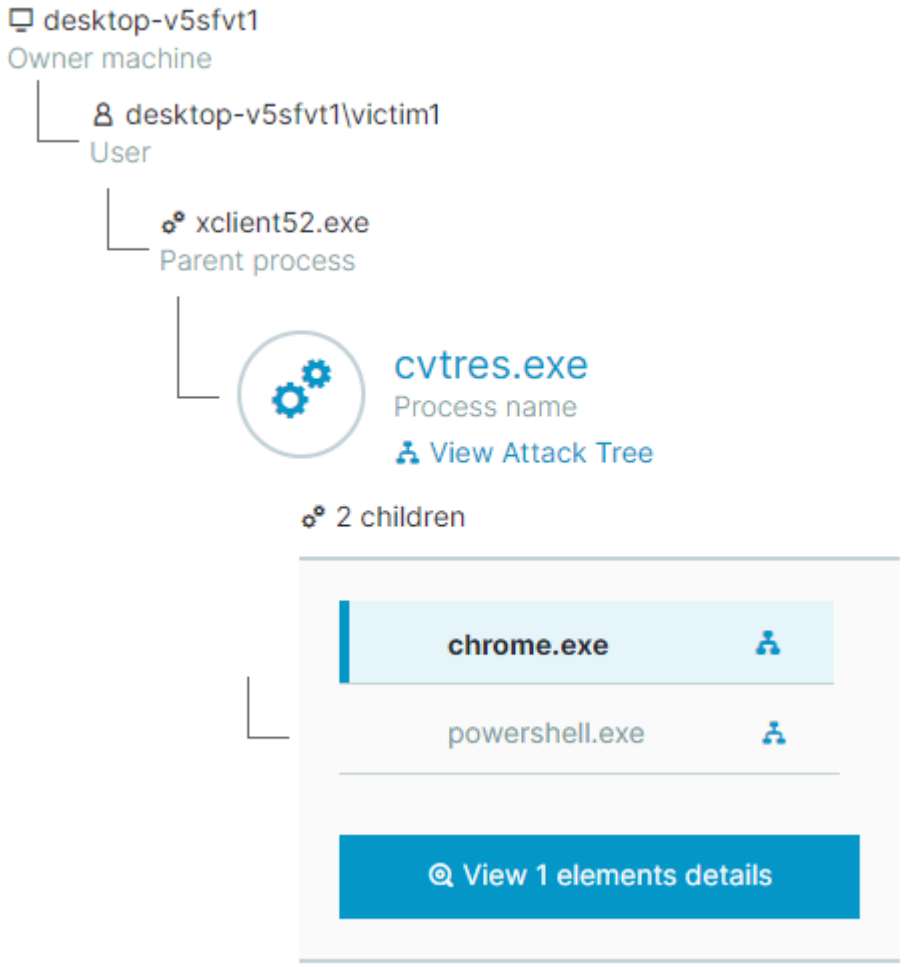
Injection To The cvtres.exe Process

During inspection, we observed that the injected *cvtres.exe* process has network connections to the remote server, which can be seen in the Process Tree.



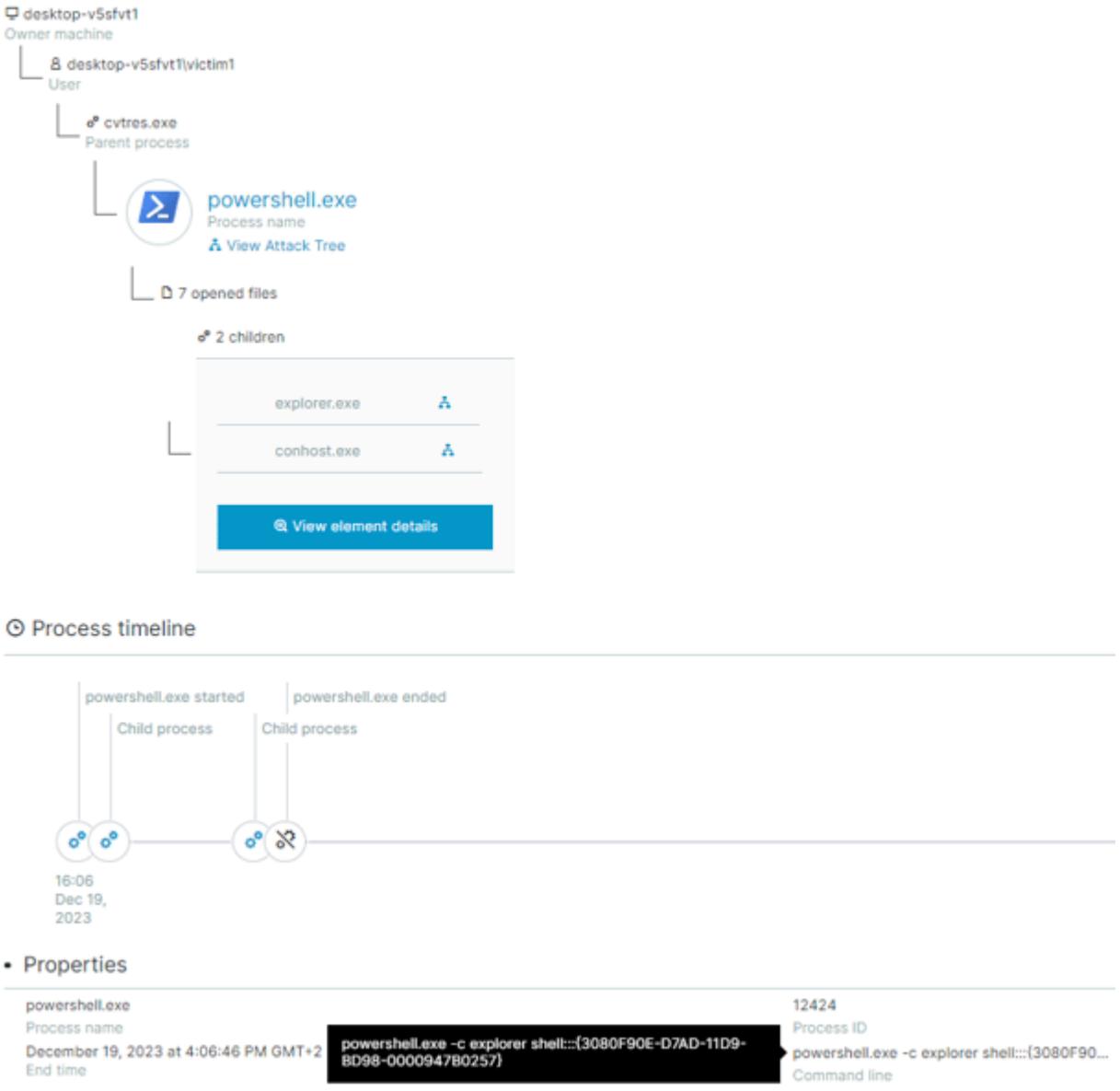
Injected cvtres.exe Running chrome.exe

hVNC Module Opens Network Connection To Remote Server To Send Victim's Unique GUID



Attack Tree Showing Injected cvtres.exe Spawning chrome.exe & powershell.exe

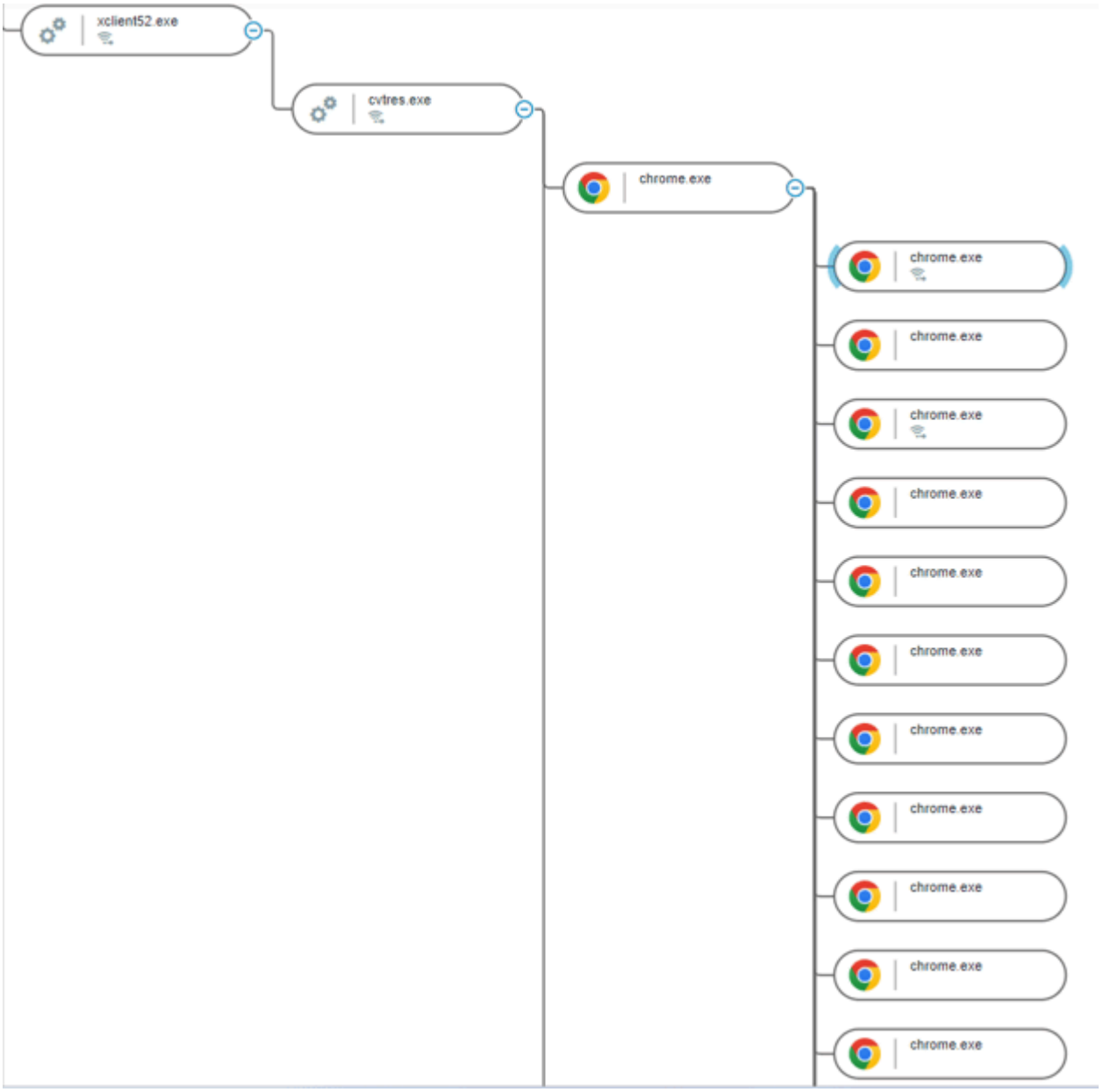
In the Cybereason Defense Platform, the Attack Tree shows *xclient52.exe* (XWorm) spawning *cvtres.exe*, spawning *powershell.exe* and *chrome.exe*, invisible from the victim's desktop.



Attack Tree For cvtres.exe

In the Cybereason Defense Platform, the Attack Tree shows *xclient52.exe* (XWorm) spawning *cvtres.exe*, spawning *powershell.exe* and *explorer.exe*, invisible from the victim's desktop.

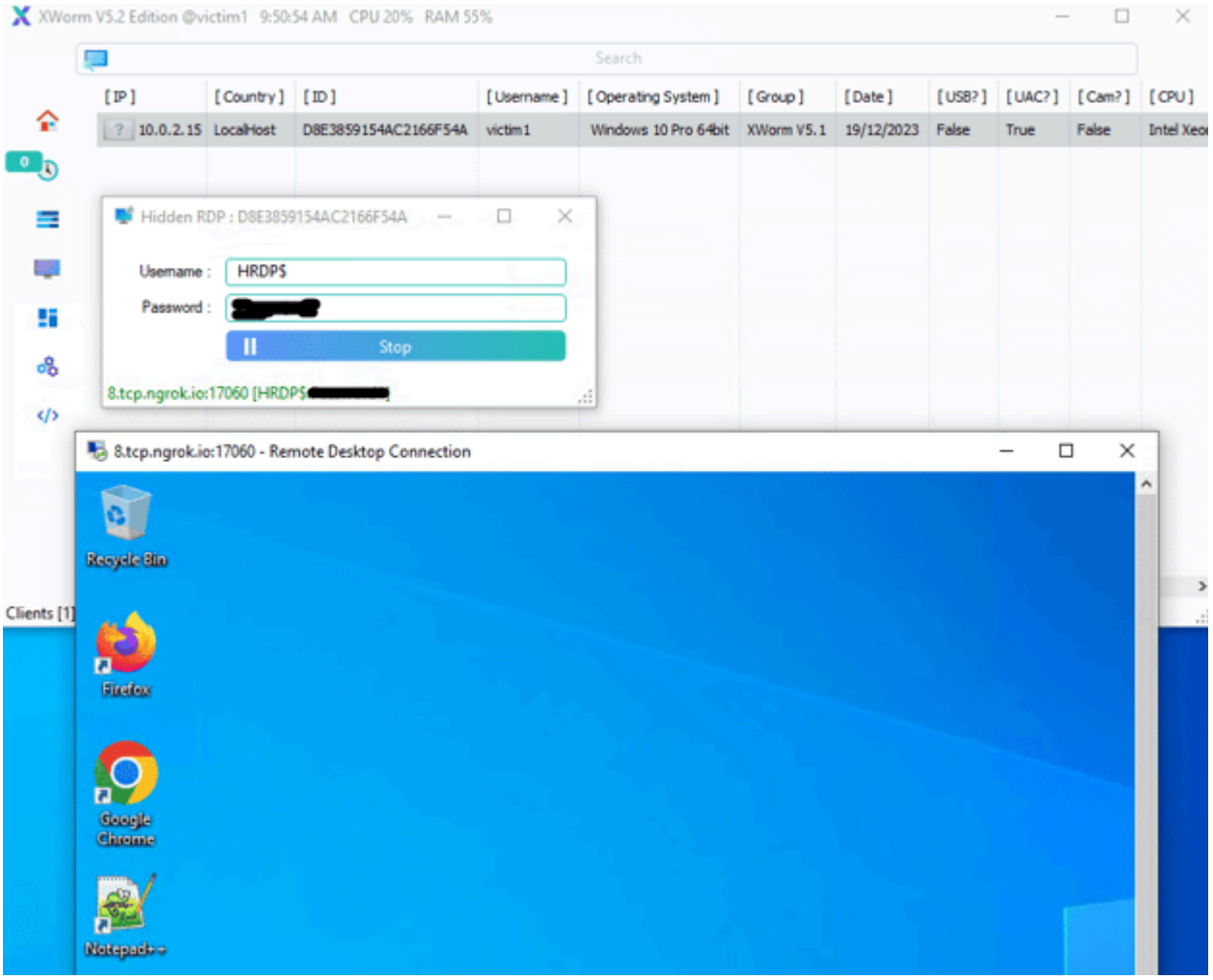
Command Line Used By XWorm Malware To Open explorer.exe Via hVNC



Attack Tree Showing Running hVNC In Memory (Without cvtres.exe Injection)

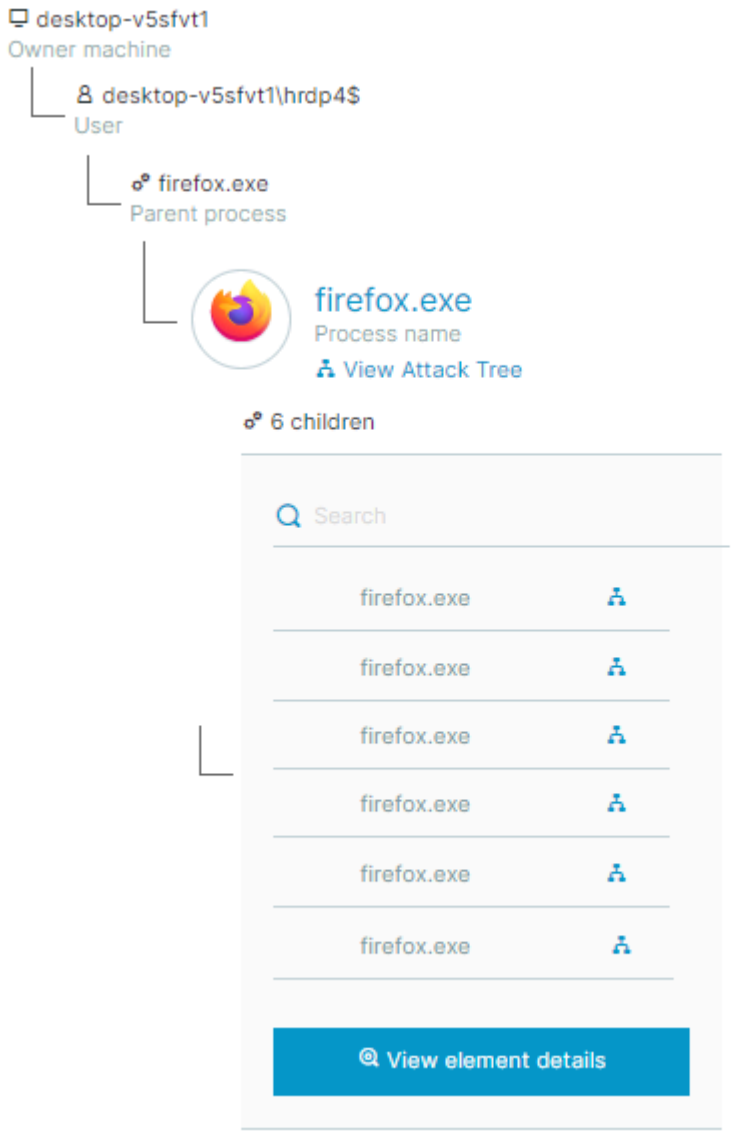
hRDP Feature (XWorm)

Finally, Cybereason analyzed the hRDP feature of XWorm, showing a successful hidden RDP connection, as shown below.



Successful hRDP Connection On The Attacker Side

The resulting process tree indicates an alternative user, HRDP4$, is the owner of the created Firefox process. The new user is created in order to use a different remote connection session than the victim to avoid visual anomalies.



New XWorm User HRDP4$ Opens firefox.exe Via hRDP

CYBEREASON SECURITY RECOMMENDATIONS

The Cybereason Defense Platform can detect and prevent payloads observed in attacks related to RATs using hVNC/hRDP features.

Cybereason Detection Of Known RATs

Additionally, the Cybereason Defense Platform can detect and prevent post-exploitation observed in attacks related to RAT using hVNC/hRDP features. In below example, *rdpwrap.dll* is used to support concurrent remote desktops.

Cybereason Detection Of rdpwrap.dll Used In hRDP

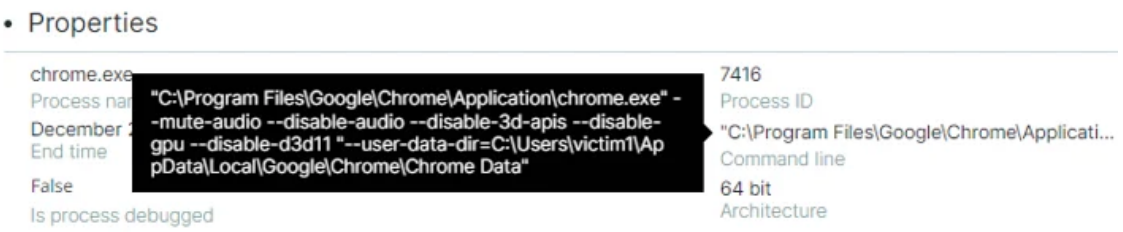
Cybereason recommends the following actions:

- Enable **Application Control** to block the execution of malicious files.
- Enable **Anti-Malware** in your environment's policies, set the Anti-Malware mode to Prevent/Disinfect.
- Enable **Variant Payload Prevention** with prevent mode on Cybereason Behavioral execution prevention.
- Enable **Variant File Prevention** with prevent mode on Cybereason Behavioral execution prevention.
- Enable **Fileless Protection** with prevent mode on Cybereason Behavioral execution prevention.
- Enable **Behavioral Execution Prevention** with prevent mode on Cybereason Behavioral execution prevention.

Detection

The following detection opportunities were identified by Cybereason:

- Multiple *explorer.exe* processes, browsers processes, *cmd.exe*, *powershell.exe* with additional Desktop handles.
- Browsers and other processes exist in the process tree but are invisible on the desktop.
- Unsigned, injected or unexpected parent processes in the process tree with browsers, **cmd**, **Powershell,** or other sensitive applications subprocesses, invisible on the desktop.
    - Ex: RAT client process *XClient52.exe* running injected Microsoft software component of Microsoft .NET Framework *cvtres.exe* with child Chrome process while chrome browser is invisible on the victim desktop but visible on the attacker desktop with option to copy victims chrome profile.
- Unexpected user with RDP access enabled in the users list.
- Internet browsers such as Chrome are running with suspicious command line parameters
    - Below are examples of command lines generated by XWorm when launching hidden browsers using the unusual flag ***-no-remote-profile*** for Firefox and ***–disable-gpu*** for Chrome.



- Below is an example of the XenoRATof XenoRAT command line generated by XWorm when launching hidden browsers using the unusual flag ***-no-remote-profile***.

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --no-sandbox --allow-no-sandbox-job
--disable-gpu --user-data-dir=C:\ChromeAutomationData
```

ABOUT THE RESEARCHER

Mark Tsipershtein, Security Researcher at Cybereason

Mark Tsipershtein, a security researcher at the Cybereason Security Research Team, focuses on research, analysis automation and infrastructure.

Mark has more than 20 years of experience in SQA, automation, and security testing.

Cybereason is dedicated to teaming with Defenders to end cyber attacks from endpoints to the enterprise to everywhere. Learn more about Cybereason XDR powered by Google Chronicle, check out our Extended Detection and Response (XDR) Toolkit, or schedule a demo today to learn how your organization can benefit from an operation-centric approach to security.

Source: https://www.cybereason.com/blog/behind-closed-doors-the-rise-of-hidden-malicious-remote-access