Cyber Intelligence Brief

September 04 - 10, 2021

See Threats. Stop Breaches. Together

*Prepared by **deepwatch Threat Intelligence Team***

Denver Office & SOC
7800 East Union Avenue, Suite 900
Denver, CO 80237 USA
855.303.3033

Purpose

This report is provided to you to improve your situational awareness and educate recipients of cyber events to aid in protecting organizations' networks, proprietary and personally identifiable information from unauthorized access, theft, or espionage. In addition, deepwatch includes additional insights and recommendations and any actions we may have taken if applicable.

Sources of Information

This publication incorporates open-source news articles to educate readers on cybersecurity matters IAW USC Title 17, section 107, Para a. All articles are truncated to avoid the appearance of copyright infringement.

Use and Definitions

To help you use this document to its full potential, a few items may be helpful to know:

- You can click on any item in the table of contents to take you to that portion of the report.
- Links throughout this document are identified by the font color of "deepwatch" Green.
- Your feedback will be extremely valuable to the deepwatch Threat Intelligence Team; please take a few minutes to send us your feedback here. Your feedback submission can be anonymous. We read each submission carefully. Feedback should be specific to your experience with this written product to enable deepwatch to make quick and continuous improvements to these products.
- Each headline will be categorized; these categories quickly let you know what the main topic of the headline is.
- Each headline this report covers includes the following information:
    - A headline, publication date, and a link to the source material.
    - Key Points section to get the most important information first.
    - Summary - This is a brief synopsis of the reporting to bring you only the most relevant information. If applicable, deepwatch will link items of interest for further context; these will be in "deepwatch" Green.
    - deepwatch Insights - This section may include additional analysis and reporting on the activity if applicable, any recommendations, and any actions deepwatch may have taken with the available information.
- If MITRE ATT&CK tactics and techniques and/or IOCs are listed, these can be found in the accompanying Appendixes.

Table of Contents

Quick Look

Data Leak | Headline: 500,000 Fortinet VPN Accounts Leaked on Underground Forum

Key Takeaway

- A list of almost 500,000 Fortinet VPN login names and passwords was leaked for free on an underground forum. "The IP addresses are for devices worldwide, with 2,959 devices located in the USA. It is believed that the Fortinet CVE-2018-13379 vulnerability was exploited to gather these credentials."

deepwatch Outlook

- deepwatch has high confidence that malicious attempts to log into Fortinet VPN devices will increase over several weeks. These devices will continue to be targeted due to being Internet-facing gateways into an organization's Network.

Ransomware | Headline: The Ideal Ransomware Victim: What Threat Actors Are Looking For

Key Takeaway

- A cyber intelligence company developed an ideal ransomware victim profile based on their observations. The typical victim is a US-based organization not in education, healthcare, government, or non-profit sectors with revenue exceeding USD 100 million. The most requested access types were for RDP, VPN, & products from Citrix, Palo Alto, VMWare, Fortinet, and Cisco.

deepwatch Outlook

- Demand for initial access brokers on cybercrime forums is growing, with more threat actors announcing they are ready to buy "access" (threat actors use this term in a very loose manner to describe multiple vectors and entry points). This is added proof of continuing organization of RaaS operations that rely on different technicians to perform their attacks.

Malware | Headline: TeamTNT Has a New Campaign Dubbed "Chimaera"

Key Takeaway

- AT&T Alien Labs has identified a new campaign by TeamTNT that has infected multiple systems. Since July 25, 2021, the campaign has been ongoing and uses various shell/batch scripts, novel open-source tools, a cryptocurrency miner, the TeamTNT IRC bot, and more.

deepwatch Outlook

- deepwatch Threat Intelligence Team has moderate confidence that this campaign will continue until more AV vendors incorporate the malware behavioral techniques and file hashes into their virus definitions.

Criminal Infrastructure | Headline: Flowspec Bulletproof Services Hosting the Cybercrime Worldwide

Key Takeaway

- Flowspec has advertised various bulletproof hosting services both underground and openly. Unfortunately, their services have been known to have facilitated phishing campaigns, ransomware, malware, Magecart skimmers, and other malicious infrastructure.

deepwatch Outlook

- Bulletproof hosting providers often provide operating space for malicious activities. deepwatch assesses with high confidence that malicious activities will source from the Bulletproof hosting provider's IP space. Flowspec has recently moved its public-facing website to the Tor Network. RiskIQ states that Flowspec's "*current IP allocation of 176.121.14.0/24 should be considered suspicious, if not out-and-out malicious.*"

Headlines

Data Leak | 500,000 Fortinet VPN Accounts Leaked on Underground Forum

September 08, 2021
Source: *Bleeping Computer*

Key Points:

- A list of almost 500,000 Fortinet VPN login names and passwords was leaked for free on an underground forum.
- The login credentials were allegedly scraped from exploitable Fortinet VPN devices last summer.
- The IP addresses are for devices worldwide, with 2,959 devices located in the USA. It is believed that the Fortinet CVE-2018-13379 vulnerability was exploited to gather these credentials."

Summary:

A list of almost 500,000 Fortinet VPN login names and passwords was leaked for free by a threat actor known as 'Orange,' the administrator of the newly launched RAMP hacking forum and a previous operator of the Babuk Ransomware operation. The login credentials were allegedly scraped from exploitable devices last summer. At the same time, a post appeared on Groove ransomware's data leak site, a relatively new ransomware operation that only has one victim currently listed on their data leak site. However, by offering freebies to the cybercriminal community, they may be hoping to recruit other threat actors to their affiliate system.

Both posts lead to a file hosted on a Tor storage server used by the Groove gang to host stolen files leaked to pressure ransomware victims to pay.

"BleepingComputer's analysis of this file shows that it contains VPN credentials for 498,908 users over 12,856 devices. Further analysis conducted by Advanced Intel shows that the IP addresses are for devices worldwide, with 2,959 devices located in the USA. Advanced Intel CTO Vitali Kremez told BleepingComputer that the Fortinet CVE-2018-13379 vulnerability was exploited to gather these credentials."

"We believe with high confidence the VPN SSL leak was likely accomplished to promote the new RAMP ransomware forum offering a "freebie" for wannabe ransomware operators." Kremez told BleepingComputer."

deepwatch Threat Intelligence Outlook

deepwatch has high confidence that malicious attempts to log into Fortinet VPN devices will increase over several weeks. These devices will continue to be targeted due to being Internet-facing gateways into an organization's Network. The vulnerability exploited to obtain the login credentials was recently featured in a CISA alert (PDF) of the top routinely exploited vulnerabilities published on July 28, 2021. deepwatch recommends organizations that use Fortinet VPNs perform a forced reset of all user passwords. deepwatch customers are encouraged to reach out to their squad manager to plan a detection strategy for malicious login attempts.

Back to Table of Contents

Ransomware | The Ideal Ransomware Victim: What Threat Actors Are Looking For

September 06, 2021
Source: *Kela*

Key Points:

- A cyber intelligence company developed an ideal ransomware victim profile based on their observations.
- The ideal victim is a US-based organization not in education, healthcare, government, or non-profit sectors with revenue exceeding USD 100 million.
- The most requested access types were for RDP, VPN, & products from Citrix, Palo Alto, VMWare, Fortinet, and Cisco.

Summary:

Kela, a cyber intelligence company, investigated who ransomware operators targeted and developed an ideal victim profile. During their research, Kela saw threat actors creating various forum posts that alleged they were ready to buy "access" and explained their requirements. The similarities between ransomware-related actors' requirements for victims and access listings and conditions for initial access brokers (IABs) demonstrate that Ransomware-as-a-Service (RaaS) operations function just like corporate entities.

Ransomware attackers look to form "industry standards" describing an ideal victim based on its revenue and geography and excluding specific sectors and countries from the targets list.

According to Kela's research, the ideal ransomware victim meets the following criteria:

- Based in the US.
- More than USD 100 million in revenue.
- Not in the education, healthcare, government, or non-profit sectors.
- Most wanted access types:
  - RDP, VPN, & products from Citrix, Palo Alto, VMWare, Fortinet, and Cisco.
  - Ransomware operators are ready to pay up to $100,000 for access.

deepwatch Threat Intelligence Outlook

Demand for IABs on cybercrime forums is growing, with more threat actors announcing they are ready to buy "access" (a term that threat actors use in a very loose manner to describe multiple vectors and entry points). This is added proof of continuing organization of RaaS operations that rely on different technicians to perform their attacks.

deepwatch has multiple detections to observe typical ransomware operations. Please coordinate with your squad manager to ensure deepwatch has the proper visibility to deploy these detections.

Back to Table of Contents

Malware | TeamTNT Has a New Campaign Dubbed "Chimaera"

September 08, 2021
Source: *AT&T*

Key Points:

- AT&T Alien Labs has identified a new campaign by TeamTNT that has infected multiple systems.
- The campaign, dubbed Chimaera, has been ongoing since July 25, 2021.
- The campaign uses multiple shell/batch scripts, novel open-source tools, a cryptocurrency miner, the TeamTNT IRC bot, and more.
- Many of the file hashes have zero or low detections in VirusTotal.

Summary:

AT&T Alien Labs has identified a new campaign by TeamTNT that has infected multiple systems. The campaign uses various shell/batch scripts, novel open-source tools, a cryptocurrency miner, the TeamTNT IRC bot, and more.

TeamTNT began running the "Chimaera" campaign using new tools. The command and control server has infection statistics that show this campaign has been running since July 25, 2021, and that it is responsible for thousands of infections globally. As of September 8, many of the file hashes have zero or low detection in VirusTotal.

One of the open-source tools used in this campaign is dubbed LaZagne, openly available on GitHub. The developer describes the project as an "*open source application used to retrieve many passwords stored on a local computer. Each software stores its passwords using different techniques (plaintext, APIs, custom algorithms, databases, etc.). This tool has been developed for the purpose of finding these passwords for the most commonly-used software.*"

deepwatch Threat Intelligence Outlook
deepwatch assesses that the low detection rates of the malware used and open-source tools like Lazagne allow TeamTNT to stay below the radar for a while. deepwatch Threat Intelligence Team has moderate confidence that this campaign will continue until more AV vendors incorporate the malware behavioral techniques and file hashes into their virus definitions.

Back to Table of Contents

Criminal Infrastructure | Flowspec Bulletproof Services Hosting the Cybercrime Worldwide

September 08, 2021
Source: *Risk IQ*

Key Points:

- Flowspec, a bulletproof hosting provider that has been around since October 2018, is a one-stop-shop for threat groups.
- Flowspec has advertised various bulletproof hosting services both underground and openly.
- Their services have been known to have facilitated phishing campaigns, ransomware, malware, Magecart skimmers, and other malicious infrastructure.

Summary:

Flowspec, a bulletproof hosting provider that has been around since October 2018, is a one-stop shop for hosting threat group infrastructure. Their services have been known to have facilitated phishing campaigns, malware delivery, Magecart skimmers, and other malicious infrastructure.

The phishing campaigns that have used Flowspec infrastructure have targeted various banks and domain names spoofing the Steam Community, Counter-Strike: Global Offensive, and Amazon. Additionally, Flowspec has hosted several Magecart domains. Also, many different malware files, including banking trojans, ransomware, various backdoors, and more, have been associated with Flowspec IP space by researchers. For example, domains resolving to Flowspec IP addresses were associated with seven ransomware files, including Ryuk, Genasom, Ergop, Ymacco, Sodinokibi, Gandcrab, and Crysis. Many of these domains have already expired or are no longer active.

Flowspec has advertised various bulletproof hosting services both underground and openly, including:

- Bulletproof servers
- Bulletproof VPS
- WAF / Bulletproof proxy
- Protected RDP
- Generation of .onion domains
- Setting up a jabber server
- Webmail
- Secure VPN
- Administration
- Cloud backup

deepwatch Threat Intelligence Outlook

Bulletproof hosting providers often provide operating space for malicious activities. deepwatch assesses with high confidence that malicious activities will source from the Bulletproof hosting provider's IP space. Flowspec has recently moved its public-facing website to the Tor Network. RiskIQ states that Flowspec's "*current IP allocation of 176.121.14.0/24 should be considered suspicious, if not out-and-out malicious.*"

Back to Table of Contents

Appendix A

Attack Vectors Featured This Week

Attack Vector Mapping Matrix		
Source	**MITRE ATT&CK Vector**	**deepwatch Detection**
TeamTNT Has a New Campaign Dubbed "Chimaera"	T1078: Valid accounts T1569: System Services T1059: Command and Scripting Interpreter T1547: Boot or Logon Autostart Execution T1053: Scheduled Task/Job T1564: Hide Artifacts T1212: Exploitation for Credential Access T1528: Steal Application Access Token T1555: Credentials from Password Stores T1210: Exploitation of Remote Services T1041: Exfiltration Over C2 Channel T1020: Automated Exfiltration T1219: Remote Access Software T1496: Resource Hijacking	deepwatch has numerous detections to observe these techniques. Please coordinate with your squad manager to plan a detection strategy and identify which techniques your squad has visibility for.

Back to Table of Contents

Appendix B

IOCs Featured This Week

Domains	
Source	**IOC**
TeamTNT Has a New Campaign Dubbed “Chimaera”	chimaera[.]cc

Hashes			
Source	**Type**	**IOC**	**Description**
TeamTNT Has a New Campaign Dubbed “Chimaera”	SHA256	caeb6eb1ee40fc4ac1da020a9a7542cffe55d29339306f6adf2d1e20e638538a	Credentials stealer, Lazagne component
	SHA256	220737c1ee400061e886eab23471f98dba38fa8e0098a018ea75d479dceece05	Malware hash
	SHA256	b6f0203ddf24cd04489cbbed24059d84504a2ba904659681ad05b7d2c130d4b5	TeamTNT IRC bot
	SHA256	fa9b38a2bd1acfd6b1b24af27cb82ea5620502d7e9cb8a913dceb897f2bcf87c	SSH lan spread
	SHA256	721d15556bd3c22f3b4c6240ff9c6d58bfa60b73b3793fa8cdc64b9e89521c5b	Malware hash
	SHA256	95809d96f85e1571a3120c7c09a7f34fa84cb5902ad5172398dc2bb0ff1dd24a	TeamTNT IRC bot
	SHA256	0ae5c1ddf91f8d5e64d58eb5395bf2216cc86d462255868e98cfb70a5a21813f	Kubernetes root PayLoad
	SHA256	f82ea98d1dc5d14817c80937b91b381e9cd29d82367a2dfbde60cfb073ea4316	Kubernetes root PayLoad
	SHA256	2d85b47cdb87a81d5fbac6000b8ee89daa1d8a3c8fbb5d2bce7a840dd348ff1d	Kubernetes setup script

	SHA256	a4000315471cf197c0552aeec0e7afbe0a935b86ff9afe5b1443812d3f7185fa	Malware hash
	SHA256	af2cf9af17f6db338ba3079b312f182593bad19fab9075a77698f162ce127758	AWS stealer
	SHA256	1b72088fc6d780da95465f80ab26ba094d89232ff30a41b1b0113c355cfffa57	Malware hash
	SHA256	3cc54142b5f88d03fb0552a655e32e94f366c9e3bb387404c6f381cfea506867	SSH lan spread
	SHA256	a46c870d1667a3ee31d2ba8969c9024bdb521ae8aad2079b672ce8416d85e8df	TeamTNT IRC bot
	SHA256	7bb1bd97dc93f0acf22eff6a5cbd9be685d18c8dbc982a24219928159c916c69	Windows component (Cryptocurrency miner setup

IP Addresses	
Source	**IOC**
TeamTNT Has a New Campaign Dubbed "Chimaera"	85.214.149[.]236
Flowspec Bulletproof Services Hosting the Cybercrime Worldwide	176.121.14.0/24

Back to Table of Contents

Feedback

Please take a few minutes to send us your feedback here. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the deepwatch Threat Operations Team. Feedback should be specific to your experience with this written product to enable deepwatch to make quick and continuous improvements to these products.

Back to Table of Contents