Mandiant APT1 samples categorized by malware families

Archived: 2026-04-06 00:52:29 UTC

Update: May 19, 2018
APT 1 resources
Threat Actor aliases:
Comment Crew, Comment Panda, PLA Unit 61398, TG-8223, APT 1, BrownFox,Group 3,GIF89a, ShadyRAT, Shanghai Group, Byzantine Candor

http://apt.threattracking.com

- 2010_11_Fireeye_VinSelf - A new backdoor in town! « VinSelf - A new backdoor in town! _ FireEye Inc.pdf
- 2010_12_Guardian_WikiLeaks cables reveal fears over Chinese cyber warfare _ US news _ The Guardian.pdf
- 2011_08_Ira Winkler _ Shady Rat Case Shows Vendors As Big a Problem As APT Itself _ CIO.pdf
- 2011_08_Kaspersky's Thoughts on Operation Shady Rat _ Nota Bene _ Eugene Kaspersky's Official Blog.pdf
- 2011_10_SANS_detailed-analysis-advanced-persistent-threat-malware-33814.pdf
- 2011_Mcafee-operation-shady-rat1.pdf
- 2012_06_Bloomberg_Hackers Linked to China's Army Seen From EU to D.C. - Bloomberg.pdf
- 2013_02_NYTimes_China's Army Is Seen as Tied to Hacking Against U.S.pdf
- 2013_03_Fireeye_TABMSGSQL and 44 WEBC2-YAHOO_The Dingo and the Baby « The Dingo and the Baby _ FireEye Inc.pdf
- 2013_05_Fireeye_APT1 Three Months Later.pdf
- 2013_05_Mandiant-APT1_Exposing One of China's Cyber Espionage Units.pdf
- 2014_05_Fireeye_The PLA and the 8_00am-5_00pm Work Day _ FireEye Confirms DOJ's Findings on APT1 Intrusion Activity « The PLA and the 8_00am-5_00pm Work Day _ FireEye Confirms DOJ's Findings on APT1 Intrusion Activity _ FireEye Inc.pdf
- 2014_06_Crowdstrike_Hat-tribution to PLA Unit 61486 ».pdf
- 2014_12_Vinself now with steganography - Airbus CyberSecurity.pdf
- 2016_BANGAT_malware-signatures_bangat.yara at master · citizenlab_malware-signatures.pdf
- GIF89a_Vinselfdecoder_malwaretracker.com _ Command and Control Decoder - Vinself Trojan.pdf
- PLA Unit 61398 _ Council on Foreign Relations Interactives.pdf

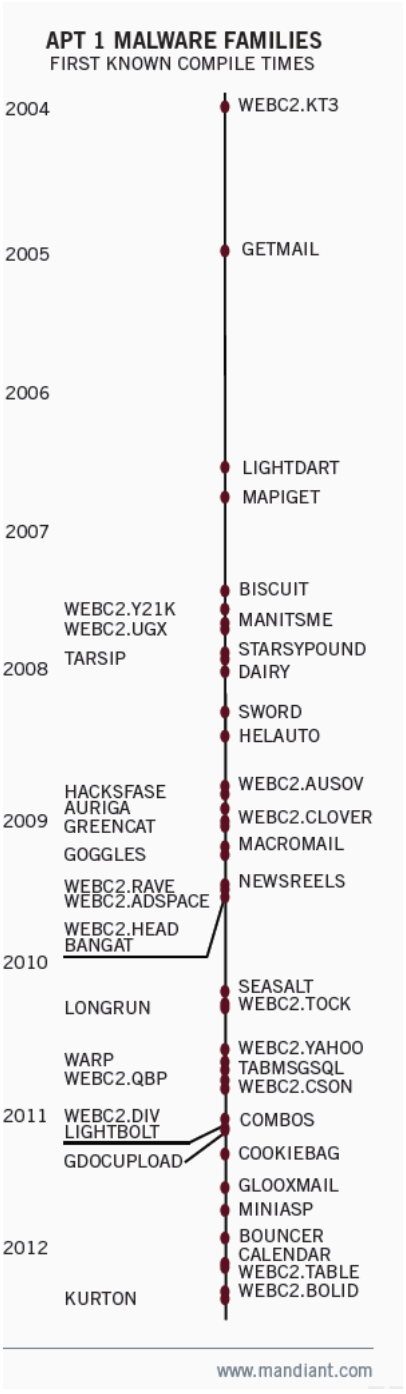
These are the samples described in the Mandiant Report APT1, in the Indicators of Compromise (IOCs). Each file is named according to the malware family, so you can run your own detection and signature tools to see how your naming convention corresponds to the one used by Mandiant.

You can use these binaries to develop signatures, compare to your samples, or study the behavior and evolution of APT1.
I added Contagio samples in several families as well.
The list of binaries and their names, as well as malware families descriptions are provided below for your convenience.

Download

Sample list and information

Below descirptions are from Mandiant IOC http://intelreport.mandiant.com/Mandiant_APT1_Report_Appendix.zip



1. AURIGA

The AURIGA malware family shares a large amount of functionality with the BANGAT backdoor. The malware family contains functionality for keystroke logging, creating and killing processes, performing file system and registry modifications, spawning interactive command shells, performing process injection, logging off the current user or shutting down the local machine. The AURIGA malware contains a driver component which is used to inject the malware DLL into other processes. This driver can also perform process and IP connection hiding. The malware family will create a copy of cmd.exe to perform its C2 activity, and replace the "Microsoft corp" strings in the cmd.exe binary with different values. The malware family typically maintains persistence through installing itself as a service.

> AURIGA_sample_6B31344B40E2AF9C9EE3BA707558C14E
> AURIGA_sample_CDCD3A09EE99CFF9A58EFEA5CCBE2BED

2. BANGAT

The BANGAT malware family shares a large amount of functionality with the AURIGA backdoor. The malware family contains functionality for keylogging, creating and killing processes, performing filesystem and registry modifications, spawning interactive command shells, performing process injection, logging off the current user or shutting down the local

machine. In addition, the malware also implements a custom VNC like protocol which sends screenshots of the desktop to the C2 server and accepts keyboard and mouse input. The malware communicates to its C2 servers using SSL, with self signed SSL certificates. The malware family will create a copy of cmd.exe to perform its C2 activity, and replace the "Microsoft corp" strings in the cmd.exe binary with different values. The malware family typically maintains persistence through installing itself as a service.

> BANGAT_sample_4C6BDDCCA2695D6202DF38708E14FC7E
> BANGAT_sample_8E8622C393D7E832D39E620EAD5D3B49
> BANGAT_sample_468FF2C12CFFC7E5B2FE0EE6BB3B239E
> BANGAT_sample_727A6800991EEAD454E53E8AF164A99C
> BANGAT_sample_BD8B082B7711BC980252F988BB0CA936
> BANGAT_sample_DB05DF0498B59B42A8E493CF3C10C578
> BANGAT_sample_E1B6940985A23E5639450F8391820655
> BANGAT_sample_EF8E0FB20E7228C7492CCDC59D87C690

Contagio samples for Bangat
Circa 2009-2010
995B44EF8460836D9091A8B361FDE489_rasauto32.dll
F10D145684BA6C71CA2D2F7EB0D89343_rasauto32.dll
43CE605B2584C27064FEBB0474A787A4_irmon32.dll
1966B265272E1660E6F340B19A7E5567_irmon32.dll
423A30C077B12354A4A5C31D4DE99689_irmon32.dll
80CA8B948409138BE40FFBC5D6D95EF1_rasauto16.dll
15138604260B1D27F92BF1EC6468B326_rasauto16.dll
616B0F00DE54D7501CEEE18823F72103_rasauto16.dll
C75D351D86DE26718A3881F62FDDDE99_irmon32.dll
E66DD357A6DFA6EBD15358E565E8F00F_irmon32.dll
0F77AF7FA673F5B3D36B926576002A1C_winhlp32.exe

3. BISCUIT

BISCUIT provides attackers with full access to an infected host. BISCUIT capabilities include launching an interactive command shell, enumerating servers on a Windows network, enumerating and manipulating process, and transferring files. BISCUIT communicates using a custom protocol, which is then encrypted using SSL. Once installed BISCUIT will attempt to beacon to its command/control servers approximately every 10 or 30 minutes. It will beacon its primary server first, followed by a secondary server. All communication is encrypted with SSL (OpenSSL 0.9.8i).

> BISCUIT_sample_5A728CB9CE56763DCCB32B5298D0F050
> BISCUIT_sample_5D8129BE965FAB8115ECA34FC84BD7F0
> BISCUIT_sample_7CB055AC3ACBF53E07E20B65EC9126A1
> BISCUIT_sample_12F25CE81596AEB19E75CC7EF08F3A38
> BISCUIT_sample_43B844C35E1A933E9214588BE81CE772
> BISCUIT_sample_70A55FDC712C6E31E013E6B5D412B0D6
> BISCUIT_sample_268EEF019BF65B2987E945AFAF29643F
> BISCUIT_sample_15901DDBCCC5E9E0579FC5B42F754FE8
> BISCUIT_sample_034374DB2D35CF9DA6558F54CEC8A455
> BISCUIT_sample_DA383CC098A5EA8FBB87643611E4BFB6

Contagio samples for
03B3CCEB253FD782590CF0EFAFD49D5F_AcroRD32.exe
8AA320A3D34CF89EF63BF801DD497490_qmqrproxy.dll

4. BOUNCER

BOUNCER will load an extracted DLL into memory, and then will call the DLL's dump export. The dump export is called with the parameters passed via the command line to the BOUNCER executable. It requires at least two arguments, the IP and port to send the password dump information. It can accept at most five arguments, including a proxy IP, port and an x.509 key for SSL authentication. The DLL backdoor has the capability to execute arbitrary commands, collect database and server information, brute force SQL login credentials, launch arbitrary programs, create processes and threads, delete files, and redirect network traffic.

> BOUNCER_sample_6EBD05A02459D3B22A9D4A79B8626BF1
> BOUNCER_sample_57353ECBAECE29ECAF8025231EB930E3
> BOUNCER_sample_CF038194F0FE222F31EC24CB80941BB1
> BOUNCER_sample_D2F1BE7E10ED39AA8BC0F7F671D824D2
> BOUNCER_sample_F90DA15F862BB8452FC51D3F0DBB3373

5. CALENDAR

This family of malware uses Google Calendar to retrieve commands and send results. It retrieves event feeds associated with Google Calendar, where each event contains commands from the attacker for the malware to perform. Results are posted back to the event feed. The malware authenticates with Google using the hard coded email address and passwords. The malware uses the deprecated ClientLogin authentication API from Google. The malware is registered as a service dll as a persistence mechanism. Artifacts of this may be found in the registry.

GCAL_sample_72d4be67abeaa6ab3827784317b1b7e9

6. COMBOS

The COMBOS malware family is an HTTP based backdoor. The backdoor is capable of file upload, file download, spawning a interactive reverse shell, and terminating its own process. The backdoor may decrypt stored Internet Explorer credentials from the local system and transmit the credentials to the C2 server. The COMBOS malware family does not have any persistence mechanisms built into itself.

> COMBOS_sample_1E3719BBF854417384A3768E4326584BCOMBOS_sample_
> EC1E62EF73D844C6C845ACDD4C1F9CE7
> COMBOS_sample_FA14D823A5D1854131DB0DC9EEF27022

his family of malware is a backdoor capable of file upload and download as well as providing remote interactive shell access to the compromised machine.

Communication with the Command & Control (C2) servers uses a combination of single-byte XOR and Base64 encoded data in the Cookie and Set-Cookie HTTP header fields. Communication with the C2 servers is over port 80. Some variants install a registry key as means of a persistence mechanism. The hardcoded strings cited include a string of a command in common with several other APT1 families.

> COOKIEBAG_sample_0C28AD34F90950BC784339EC9F50D288
> COOKIEBAG_sample_321D75C9990408DB812E5A248A74F8C8
> COOKIEBAG_sample_543E03CC5872E9ED870B2D64363F518B
> COOKIEBAG_sample_989B797C2A63FBFC8E1C6E8A8CCD6204
> COOKIEBAG_sample_57326CD78A56D26E349BBD4BCC5B9FA2
> COOKIEBAG_sample_DB2580F5675F04716481B24BB7AF468E
> COOKIEBAG_sample_F3611C5C793F521F7FF2A69C22D4174E

7 DAIRY

Members of this malware family are backdoors that provide file downloading, process listing, process killing, and reverse shell capabilities. This malware may also add itself to the Authorized Applications list for the Windows Firewall.

> DAIRY_sample_995442F722CC037885335340FC297EA0

8. GETMAIL

Members of this family of malware are utilities designed to extract email messages and attachments from Outlook PST files. One part of this utility set is an executable, one is a dll. The malware may create a registry artifact related to the executable.

> GETMAIL_sample_909BEF6DB8D33854E983EBCCDD71419F
> GETMAIL_sample_E81DB0198D2A63C4CCFC33F58FCB821E
> GETMAIL_sample_E212AAF642D73A2E4A885F12EEA86C58

9. GDOCUPLOAD

This family of malware is a utility designed to upload files to Google Docs. Nearly all communications are with docs.google.com are SSL encrypted. The malware does not use Google's published API to interact with their services. The malware does not currently work with Google Docs. It does not detect HTTP 302 redirections and will get caught in an infinite loop attempting to parse results from Google that are not present.

> GDOCUPLOAD-sample_232d1be2d8cbbd1cf57494a934628504

10 GLOOXMAIL - aka TROJAN.GTALK http://www.cyberengineeringservices.com/trojan-gtalk/

GLOOXMAIL communicates with Google's Jabber/XMPP servers and authenticates with a hard-coded username and password. The malware can accept commands over XMPP that includes file upload and download, provide a remote shell, sending process listings, and terminating specified processes. The malware makes extensive use of the open source gloox

library (http://camaya.net/gloox/, version 0.9.9.12) to communicate using the Jabber/XMPP protocol. All communications with the Google XMPP server are encrypted.

> GLOOXMAIL_sample_3DE1BD0F2107198931177B2B23877DF4
> GLOOXMAIL_sample_15A33F8FE11B94BDD38BFF651F6A5CD1

A family of downloader malware, that retrieves an encoded payload from a fixed location, usually in the form of a file with the .jpg extension. Some variants have just an .exe that acts as a downloader, others have an .exe launcher that runs as a service and then loads an associated .dll of the same name that acts as the downloader. This IOC is targeted at the downloaders only. After downloading the file, the malware decodes the downloaded payload into an .exe file and launches it. The malware usually stages the files it uses in the %TEMP% directory or the %WINDIR%\Temp directory.

> GOGGLES_sample_09D372E4259980AC95FDADF1846578D9
> GOGGLES_sample_57F98D16AC439A11012860F88DB21831
> GOGGLES_sample_51326BF40DA5A5357A143DD9A6E6A11C
> GOGGLES_sample_A5B581C0600815B1112CA2FED578928B
> GOGGLES_sample_BCB087F69792B69494A3EDAD51A842BB
> GOGGLES_sample_BF80DBF969B73790253F683CD723FD71
> GOGGLES_sample_DB50416D9E67F4982E89E0FFB0ADE6F3

12 GREENCAT

Members of this family are full featured backdoors that communicates with a Web-based Command & Control (C2) server over SSL. Features include interactive shell, gathering system info, uploading and downloading files, and creating and killing processes, Malware in this family usually communicates with a hard-coded domain using SSL on port 443. Some members of this family rely on launchers to establish persistence mechanism for them. Others contains functionality that allows it to install itself, replacing an existing Windows service, and uninstall itself. Several variants use %SystemRoot%\Tasks or %WinDir%\Tasks as working directories, additional malware artifacts may be found there.

> GREENCAT_sample_0C5E9F564115BFCBEE66377A829DE55F
> GREENCAT_sample_1F92FF8711716CA795FBD81C477E45F5
> GREENCAT_sample_3E6ED3EE47BCE9946E2541332CB34C69
> GREENCAT_sample_3E69945E5865CCC861F69B24BC1166B6
> GREENCAT_sample_5AEAA53340A281074FCB539967438E3F
> GREENCAT_sample_6D2320AF561B2315C1241E3EFD86067F
> GREENCAT_sample_30E78D186B27D2023A2A7319BB679C3F
> GREENCAT_sample_36C0D3F109AEDE4D76B05431F8A64F9E
> GREENCAT_sample_55FB1409170C91740359D1D96364F17B
> GREENCAT_sample_57E79F7DF13C0CB01910D0C688FCD296
> GREENCAT_sample_120C2E085992FF59A21BA401EC29FEC9_different
> GREENCAT_sample_390D1F2A620912104F53C034C8AEF14B
> GREENCAT_sample_871CC547FEB9DBEC0285321068E392B8
> GREENCAT_sample_7388D67561D0A7989202AD4D37EFF24F
> GREENCAT_sample_A99E06E2F90DB4E506EF1347A8774DD5
> GREENCAT_sample_A565682D8A13A5719977223E0D9C7AA4
> GREENCAT_sample_AB208F0B517BA9850F1551C9555B5313
> GREENCAT_sample_B3BC979D8DE3BE09728C5DE1A0297C4B
> GREENCAT_sample_B5E9CE72771217680EFAEECFAFE3DA3F
> GREENCAT_sample_B8F61242E28F2EDF6CB1BE8781438491
> GREENCAT_sample_BA0C4D3DBF07D407211B5828405A9B91
> GREENCAT_sample_C044715C2626AB515F6C85A21C47C7DD
> GREENCAT_sample_E54CE5F0112C9FDFE86DB17E85A5E2C5
> GREENCAT_sample_E83F60FB0E0396EA309FAF0AED64E53F
> GREENCAT_sample_F4ED3B7A8A58453052DB4B5BE3707342
> GREENCAT_sample_FAB6B0B33D59F393E142000F128A9652

13. HACKFASE

This family of malware is a backdoor that provides reverse shell, process creation, system statistics collection, process enumeration, and process termination capabilities.

This family is designed to be a service DLL and does not contain an installation mechanism.

It usually communicates over port 443. Some variants use their own encryption, others use SSL.

> HACKFASE_sample_0D0240672A314A7547D328F824642DA8
> HACKFASE_sample_1A0C7E61BCC50D57B7BCF9D9AF691DE5
> HACKFASE_sample_9E860622FEE66074DFE81DCFCC40C4E2

> HACKFASE_sample_17199DDAC616938F383A0339F416C890
> HACKFASE_sample_BCBDEF1678049378BE04719ED29078D2

14. HELAUTO

This family of malware is designed to operate as a service and provides remote command execution and file transfer capabilities to a fixed IP address or domain name. All communication with the C2 server happens over port 443 using SSL.

This family can be installed as a service DLL. Some variants allow for uninstallation.

> HELAUTO_sample_47E7F92419EB4B98FF4124C3CA11B738
> HELAUTO_sample_DA6B0EE7EC735029D1FF4FA863A71DE8

15. KURTON

This family of malware is a backdoor that tunnels its connection through a preconfigured proxy. The malware communicates with a remote command and control server over HTTPS via the proxy. The malware installs itself as a Windows service with a service name supplied by the attacker but defaults to IPRIP if no service name is provided during install.

No Mandiant samples available.

These are Contagio samples dated 2009

57C69FECFECDCB5288687DF2AC96E44F_iprinp.dll

7C136A9E8D94BF117288D9B5388019D6_iprinp.dll

82C39E6979022E57B93B719793B39A30_iprinp.dll

A327B9D97CA479B89297F438F87816A0_iprinp.dll

A6C1595BD7B1A85C42FBD674460DC35D_iprinp.dll

15. LIGHTBOLT

LIGHTBOLT is a utility with the ability to perform HTTP GET requests for a list of user-specified URLs. The responses of the HTTP requests are then saved as MHTML files, which are added to encrypted RAR files. LIGHTBOLT has the ability to use software certificates for authentication.

> LIGHTBOLT_sample_2E86A9862257A0CF723CEEF3868A1A12

16 LIGHTDART

LIGHTDART is a tool used to access a pre-configured web page that hosts an interface to query a database or data set. The tool then downloads the results of a query against that web page to an encrypted RAR file. This RAR file (1.rar) is renamed and uploaded to an attacker controlled FTP server, or uploaded via an HTTP POST with a .jpg extension. The malware will execute this search once a day. The target webpage usually contains information useful to the attacker, which is updated on a regular basis. Examples of targeted information include weather information or ship coordinates.

No samples

17. LONGRUN

LONGRUN is a backdoor designed to communicate with a hard-coded IP address and provide the attackers with a custom interactive shell. It supports file uploads and downloads, and executing arbitrary commands on the compromised machine. When LONGRUN executes, it first loads configuration data stored as an obfuscated string inside the PE resource section. The distinctive string thequickbrownfxjmpsvalzydg is used as part of the input to the decoding algorithm. When the configuration data string is decoded it is parsed and treated as an IP and port number. The malware then connects to the host and begins interacting with it over a custom protocol.

No samples

18. MANITSME

This family of malware will beacon out at random intervals to the remote attacker. The attacker can run programs, execute arbitrary commands, and easily upload and download files. This IOC looks for both the dropper file and the backdoor.

> MANITSME_sample_e97ebb5b2050b86999c55797c2348ba7

This malware utility is a set of two files that operate in conjunction to extract email messages and attachments from an Exchange server. In order to operate successfully, these programs require authentication credentials for a user on the Exchange server, and must be run from a machine joined to the domain that has Microsoft Outlook installed (or equivalent software that provides the Microsoft 'Messaging API' (MAPI) service).

> MAPIGET_sample_C627E595C9EC6DC2199447AEAB59AC03
> MAPIGET_sample_F3C6C797EF80787E6CBEEAA77496A3CB

Contagio samples for MAPIGET

09E25BB934D8523FCCD27B86FBF4F8CE_m.exe
C57902ACE7FF4173AE41F1292EA85E2A_MAPI.exe

20. MINIASP

This family of malware consists of backdoors that attempt to fetch encoded commands over HTTP. The malware is capable of downloading a file, downloading and executing a file, executing arbitrary shell commands, or sleeping a specified interval.

> MINIASP_77FBFED235D6062212A3E43211A5706E
> MINIASP_81B03CBCFC4B9D090CD8F5E5DA816895
> MINIASP_E476E4A24F8B4FF4C8A0B260AA35FC9F

21 NEWSREELS

The NEWSREELS malware family is an HTTP based backdoor. When first started, NEWSREELS decodes two strings from its resources section. These strings are both used as C2 channels, one URL is used as a beacon URL (transmitting) and the second URL is used to get commands (receiving). The NEWSREELS malware family is capable of performing file uploads, downloads, creating processes or creating an interactive reverse shell.

> NEWSREELS_sample_02C65973B6018F5D473D701B3E7508B2
> NEWSREELS_sample_2C49F47C98203B110799AB622265F4EF
> NEWSREELS_sample_270D42F292105951EE81E4085EA45054
> NEWSREELS_sample_0496E3B17CF40C45F495188A368C203A
> NEWSREELS_sample_523F56515221161579EE6090C962E5B1
> NEWSREELS_sample_933B11BC4799F8D9F65466FB2E3EA659
> NEWSREELS_sample_A2CD1189860B9BA214421AAB86ECBC8A
> NEWSREELS_sample_A639F598D4C0B9AA7A4691D05F27D977
> NEWSREELS_sample_AF2F7B070245C90BD2A0A0845314173A
> NEWSREELS_sample_B8277CCE81E0A372BC35D33A0C9483C2
> NEWSREELS_sample_BAABD9B76BFF84ED27FD432CFC6DF241
> NEWSREELS_sample_D4C7F1F80883412F9796F1270ACCFF50
> NEWSREELS_sample_D271AE0F4E9230AF3B61EAFE7F671FDE
> NEWSREELS_sample_EF6C375E3E6930E2B50E1E97FE6FBCC9

22. SEASALT

The SEASALT malware family communicates via a custom binary protocol. It is capable of gathering some basic system information, file system manipulation, file upload and download, process creation and termination, and spawning an interactive reverse shell. The malware maintains persistence by installing itself as a service.

> SEASALT_sample_5E0DF5B28A349D46AC8CC7D9E5E61A96
> SEASALT_sample_F0726AADCF5D66DAF528F79BA8507113

23. STARSYPOUND

STARSYPOUND provides an interactive remote shell over an obfuscated communications channel. When it is first run, it loads a string (from the executable PE resource section) containing the beacon IP address and port. The malware sends the beacon string "*(SY)# <HOSTNAME>" to the remote system, where <HOSTNAME> is the hostname of the victim system. The remote host responds with a packet that also begins with the string "*(SY)# cmd". This causes the malware to launch a new cmd.exe child process. Further communications are forwarded to the cmd.exe child process to execute. The commands sent to the shell and their responses are obfuscated when sent over the network.

> STARSYPOUND_sample_2BA0D0083976A5C1E3315413CDCFFCD2STARSYPOUND_sample_2DD892986B2249B5214639ECC8AC0223STAR

24. SWORD

This family of malware provides a backdoor over the network to the attackers. It is configured to connect to a single host and offers file download over HTTP, program execution, and arbitrary execution of commands through a cmd.exe instance.

> SWORD_sample_052F5DA1734464A985DCD669BFF62F93

This malware family is a full-featured backdoor capable of file uploading and downloading, arbitrary execution of programs, and providing a remote interactive command shell.

All communications with the C2 server are sent over HTTP to a static URL, appending various URL parameters to the request. Some variants use a slightly different URL.

> TABMSGSQL_sample_001DD76872D80801692FF942308C64E6
> TABMSGSQL_sample_2F930D92DC5EBC9D53AD2A2B451EBF65
> TABMSGSQL_sample_3E87051B1DC3463F378C7E1FE398DC7D
> TABMSGSQL_sample_8A86DF3D382BFD1E4C4165F4CACFDFF8
> TABMSGSQL_sample_052EC04866E4A67F31845D656531830D
> TABMSGSQL_sample_002325A0A67FDED0381B5648D7FE9B8E
> TABMSGSQL_sample_55886D571C2A57984EA9659B57E1C63A

Contagio sample for TABMSDSQL - LETSGO

DC1286AAC46B0EAD7B27F045E5B09EFF Conference Materials.zip (dropper)

26. TARSIP-ECLIPSE

The TARSIP malware family is a backdoor which communicates over encoded information in HTTPS headers. Typical TARSIP malware samples will only beacon out to their C2 servers if the C2 DNS address resolves to a specific address. The capability of TARSIP backdoors includes file uploading, file downloading, interactive command shells, process enumeration, process creation, process termination. The TARSIP-ECLIPSE family is distinguished by the presence of 'eclipse' in .pdb debug strings present in the malware samples. It does not provide a built in mechanism to maintain persistence.

> TARSIP-ECLIPSE_sample_0B506C6DDE8D07F9EEB82FD01A6F97D4
> TARSIP-ECLIPSE_sample_4A54D7878D4170C3D4E3C3606365C42C
> TARSIP-ECLIPSE_sample_4F763B07A7B8A80F1F9408E590F79532
> TARSIP-ECLIPSE_sample_3107DE21E480AB1F2D67725F419B28D0
> TARSIP-ECLIPSE_sample_8934AEED5D213FE29E858EEE616A6EC7
> TARSIP-ECLIPSE_sample_123505024F9E5FF74CB6AA67D7FCC392
> TARSIP-ECLIPSE_sample_CA327BC83FBE38B3689CD1A5505DFC33

27. TARSIP-MOON

The TARSIP malware family is a backdoor which communicates over encoded information in HTTPS headers. Typical TARSIP malware samples will only beacon out to their C2 servers if the C2 DNS address resolves to a specific address. The capability of TARSIP backdoors includes file uploading, file downloading, interactive command shells, process enumeration, process creation, process termination. The TARSIP-MOON family is distinguished by the presence of 'moon' in .pdb debug strings present in the malware samples. It does not provide a built in mechanism to maintain persistence.

> TARSIP-MOON_sample_2BD02B41817D227058522CCA40ACD390
> TARSIP-MOON_sample_95F25D3AFC5370F5D9FD8E65C17D3599
> TARSIP-MOON_sample_0908D8B3E459551039BADE50930E4C1B
> TARSIP-MOON_sample_6808EC6DBB23F0FA7637C108F44C5C80
> TARSIP-MOON_sample_A5D4EBC0285F0213E0C29D23BC410889
> TARSIP-MOON_sample_C91EACAB7655870764D13BA741AA9A73

28. WARP

The WARP malware family is an HTTP based backdoor written in C++, and the majority of its code base is borrowed from source code available in the public domain. Network communications are implemented using the same WWW client library (w3c.cpp) available from www.dankrusi.com/file_69653F3336383837.html. The malware has system survey functionality (collects hostname, current user, system uptime, CPU speed, etc.) taken directly from the BO2K backdoor available from www.bo2k.com. It also contains the hard disk identification code found at www.winsim.com/diskid32/diskid32.cpp. When the WARP executing remote commands, the malware creates a copy of the ?%SYSTEMROOT%\system32\cmd.exe? file as '%USERPROFILE%\Temp\~ISUN32.EXE'. The version signature information of the duplicate executable is zeroed out. Some WARP variants maintain persistence through the use of DLL search order hijacking.

no sample

29 WEBC2-ADSPACE

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. This family of malware is capable of downloading and executing a file. All variants represented here are the same file with different MD5 signatures. This malware attempts to contact its C2 once a week (Thursday at 10:00 AM). It looks for commands inside a set of HTML tags, part of which are in the File Strings indicator term below.

> WEBC2-ADSPACE_sample_AB00B38179851C8AA3F9BC80ED7BAA23

30. WEBC2-AUSOV

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. This malware family is a only a downloader which operates over the HTTP protocol with a hard-coded URL. If directed, it has the capability to download, decompress, and execute compressed binaries.

> WEBC2-AUSOV_sample_6E442C5EF460BEE4C9457C6BF7A132D6
> WEBC2-AUSOV_sample_097B5ABB53A3D84FA9EABDA02FEF9E91
> WEBC2-AUSOV_sample_A40E20FF8B991308F508239625F275D8
> WEBC2-AUSOV_sample_D262CB8267BEB0E218F6D11D6AF9052E

31 WEBC2-BOLID

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. This family of malware is a backdoor capable of downloading files and updating its configuration.

Communication with the command and control (C2) server uses a combination of single-byte XOR and Base64 encoded data wrapped in standard HTML tags. The malware family installs a registry key as a persistence mechanism.

> WEBC2-BOLID_sample_1EA61A0945BDE3C6F41E12BC01928D37
> WEBC2-BOLID_sample_5FF3269FACA4A67D1A4C537154AAAD4B
> WEBC2-BOLID_sample_53B263DD41838AA178A5CED338A207F3
> WEBC2-BOLID_sample_9675827A495F4BA6A4EFD4DD70932B7C
> WEBC2-BOLID_sample_D8238E950608E5ABA3D3E9E83E9EE2CC

32. WEBC2-CLOVER

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The family of malware provides the attacker with an interactive command shell, the ability to upload and download files, execute commands on the system, list processes and DLLs, kill processes, and ping hosts on the local network. Responses to these commands are encrypted and compressed before being POSTed to the server. Some variants copy cmd.exe to Updatasched.exe in a temporary directory, and then may launch that in a process if an interactive shell is called. On initial invocation, the malware also attempts to delete previous copies of the Updatasched.exe file.

> WEBC2-CLOVER_sample_2FCCAA39533DE02490B1C6395878DD79
> WEBC2-CLOVER_sample_29C691978AF80DC23C4DF96B5F6076BB
> WEBC2-CLOVER_sample_065E63AFDFA539727F63AF7530B22D2F

33. WEBC2-CSON

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. Members of this family of malware act only as downloaders and droppers for other malware. They communicate with a hard-coded C2 server, reading commands embedded in HTML comment fields. Some variants are executables which act upon execution, others are DLLs which can be attached to services or loaded through search order hijacking.

> WEBC2-CSON_sample_7D3140BD028F70F1FA865364B69C5999
> WEBC2-CSON_sample_50F35B7C86AEDE891A72FCB85F06B0B7
> WEBC2-CSON_sample_73D125F84503BD87F8142CF2BA8AB05E
> WEBC2-CSON_sample_575836EBB1B8849F04E994E9160370E4
> WEBC2-CSON_sample_4192479B055B2B21CB7E6C803B765D34
> WEBC2-CSON_sample_277964807A66AEEB6BD81DBFCAA3E4E6
> WEBC2-CSON_sample_A38A367D6696BA90B2E778A5A4BF98FD
> WEBC2-CSON_sample_D22863C5E6F098A4B52688B021BEEF0A
> WEBC2-CSON_sample_F1E5D9BF7705B4DC5BE0B8A90B73A863
> WEBC2-CSON_sample_F802B6E448C054C9C16B97FF85646825

34. WEBC2-DIV

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-DIV variant searches for the strings "div safe:" and " balance" to delimit encoded C2 information. If the decoded string begins with the letter "J" the malware will parse additional arguments in the decoded string to specify the sleep interval to use. WEBC2-DIV is capable of downloading a file, downloading and executing a file, or sleeping a specified interval.

> WEBC2-DIV_sample_1E5EC6C06E4F6BB958DCBB9FC636009D

35 WEBC2-GREENCAT

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. This malware is a variant on the GREENCAT family, using a fixed web C2. This family is a full featured backdoor which provides remote command execution, file transfer, process and service enumeration and manipulation. It installs itself persistently through the current user's registry Run key.

> WEBC2-GREENCAT_sample_1CE4605E771A04E375E0D1083F183E8E
> WEBC2-GREENCAT_sample_36C0D3F109AEDE4D76B05431F8A64F9E
> WEBC2-GREENCAT_sample_55FB1409170C91740359D1D96364F17B
> WEBC2-GREENCAT_sample_BA0C4D3DBF07D407211B5828405A9B91
> WEBC2-GREENCAT_sample_E54CE5F0112C9FDFE86DB17E85A5E2C5
> WEBC2-GREENCAT_sample_E83F60FB0E0396EA309FAF0AED64E53F

36. WEBC2-HEAD

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-HEAD variant communicates over HTTPS, using the system's SSL implementation to encrypt all communications with the C2 server. WEBC2-HEAD first issues an HTTP GET to the host, sending the Base64-encoded string containing the name of the compromised machine running the malware.

> WEBC2-HEAD_sample_7B42B35832855AB4FF37AE9B8FA9E571
> WEBC2-HEAD_sample_88C7C50CD4130561D57A1D3B82C5B953
> WEBC2-HEAD_sample_165EF79E7CAA806F13F82CC2BBF3DEDD
> WEBC2-HEAD_sample_649D54BC9EEF5A60A4B9D8B889FEE139
> WEBC2-HEAD_sample_973F4A238D6D19BDC7B42977B07B9CEF
> WEBC2-HEAD_sample_B74022A7B9B63FDC541AE0848B28A962
> WEBC2-HEAD_sample_C4C638750526E28F68D6D71FD1266BDF
> WEBC2-HEAD_sample_C9172B3E83C782BC930C06B628F31FA5
> WEBC2-HEAD_sample_EC8C89AA5E521572C74E2DD02A4DAF78
> WEBC2-HEAD_sample_F627990BBE2EC5C48C180F724490C332

37 WEBC2-KT3

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-KT3 variant searches for commands in a specific comment tag. Network traffic starting with *!Kt3+v| may indicate WEBC2-KT3 activity.

> WEBC2-KT3_sample_EC3A2197CA6B63EE1454D99A6AE145AB

38 WEBC2-QBP

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-QBP variant will search for two strings in a HTML comment. The first will be "2010QBP " followed by " 2010QBP//--". Inside these tags will be a DES-encrypted string.

> WEBC2-QBP_sample_929802A27737CEBC59D19DA724FDF30A
> WEBC2-QBP_sample_C04C796EF126AD7429BE7D55720FE392
> WEBC2-QBP_sample_CF9C2D5A8FBDD1C5ADC20CFC5E663C21

39 WEBC2-RAVE

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. This family of malware will set itself up as a service and connect out to a hardcoded web page and read a modified base64 string from this webpage. The later versions of this malware supports three commands (earlier ones are just downloaders or reverse shells). The first commands will sleep the malware for N number of hours. The second command will download a binary from the encoded HTML comment and execute it on the infected host. The third will spawn an encoded reverse shell to an attacker specified location and port.

> WEBC2-RAVE_sample_5BCAA2F4BC7567F6FFD5507A161E221A
> WEBC2-RAVE_sample_9F11BC08AF048C5C3A110E567082FE0B

> WEBC2-RAVE_sample_438983192903F3FECF77500A39459EE6
> WEBC2-RAVE_sample_A2534E9B7E4146368EA3245381830EB0
> WEBC2-RAVE_sample_BDD2AD4C0E1E5667D117810AE9E36C4B
> WEBC2-RAVE_sample_BF0EE4367EA32F8E3B911C304258E439

40. WEBC2-TABLE

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-TABLE variant looks for web pages containing 'background', 'align', and 'bgcolor' tags to be present in the requested Web page. If the data in these tags are formatted correctly, the malware will decode a second URL and a filename. This URL is then retrieved, written to the decoded filename and executed.

> WEBC2-TABLE_sample_7A7A46E8FBC25A624D58E897DEE04FFA

41 WEBC2-TOCK

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-TOCK variant looks for tags which include the name of the system in them as a parameter. If those tags are formed correctly, the malware will decode the payload URL from the web page, then download and execute the payload.

no samples

42. WEBC2-UGX

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. Members of this family of malware provide remote command shell and remote file download and execution capabilities.
The malware downloads a web page containing a crafted HTML comment that subsequently contains an encoded command. The contents of this command tell the malware whether to download and execute a program, launch a reverse shell to a specific host and port number, or to sleep for a period of time.

> WEBC2-UGX_sample_4B19A2A6D40A5825E868C6EF25AE445E
> WEBC2-UGX_sample_54D5D171A482278CC8EACF08D9175FD7
> WEBC2-UGX_sample_56DE2854EF64D869B5DF7AF5E4EFFE3E
> WEBC2-UGX_sample_75DAD1CCABAE8ADEB5BAE899D0C630F8
> WEBC2-UGX_sample_8462A62F13F92C34E4B89A7D13A185AD

43. WEBC2-Y21K

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. Members of this family of backdoor malware talk to specific Web-based Command & Control (C2) servers. The backdoor has a limited command set, depending on version. It is primarily a downloader, but it classified as a backdoor because it can accept a limited command set, including changing local directories, downloading and executing additional files, sleeping, and connecting to a specific IP & port not initially included in the instruction set for the malware. Each version of the malware has at least one hardcoded URL to which it connects to receive its initial commands. This family of malware installs itself as a service, with the malware either being the executable run by the service, or the service DLL loaded by a legitimate service. The same core code is seen recompiled on different dates or with different names, but the same functionality. Key signatures include a specific set of functions (some of which can be used with the OS-provided rundll32.exe tool to install the malware as a service), and hardcoded strings used in communication with C2 servers to issue commands to the implant.

> WEBC2-Y21K_sample_4CABFAEF26FD8E5AEC01D0C4B90A32F3
> WEBC2-Y21K_sample_225E33508861984DD2A774760BFDFC52
> WEBC2-Y21K_sample_2479A9A50308CB72FCD5E4E18EF06468

44. WEBC2-YAHOO

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-YAHOO variant enters a loop where every ten minutes it attempts to download a web page that may contain an encoded URL. The encoded URL will be found in the pages returned inside an attribute named 'sb' or 'ex' within a tag named 'yahoo'. The embedded link can direct the malware to download and execute files.

> WEBC2-YAHOO_sample_2B659D71AE168E774FAAF38DB30F4A84
> WEBC2-YAHOO_sample_4C9C9DBF388A8D81D8CFB4D3FC05F8E4
> WEBC2-YAHOO_sample_7A670D13D4D014169C4080328B8FEB86
> WEBC2-YAHOO_sample_36D5C8FC4B14559F73B6136D85B94198

> WEBC2-YAHOO_sample_37DDD3D72EAD03C7518F5D47650C8572
> WEBC2-YAHOO_sample_0149B7BD7218AAB4E257D28469FDDB0D
> WEBC2-YAHOO_sample_1415EB8519D13328091CC5C76A624E3D
> WEBC2-YAHOO_sample_A8F259BB36E00D124963CFA9B86F502E
> WEBC2-YAHOO_sample_AA4F1ECC4D25B33395196B5D51A06790
> WEBC2-YAHOO_sample_CC3A9A7B026BFE0E55FF219FD6AA7D94
> WEBC2-YAHOO_sample_F7F85D7F628CE62D1D8F7B39D8940472
