# Say “Cheese”: WebMonitor RAT Comes with C2-as-a-Service (C2aaS)

researchcenter.paloaltonetworks.com/2018/04/unit42-say-cheese-webmonitor-rat-comes-c2-service-c2aas/

Mike Harbison, Simon Conant April 13, 2018

By Mike Harbison and Simon Conant

April 13, 2018 at 5:00 AM

Category: Unit 42

Tags: C2aaS, RAT, WebMonitor


While looking at commodity RATs currently offered on underground forums, we came across “WebMonitor”, on the market since mid-2017. We noticed that while detection was high for most anti-virus vendors, all tagged it with only generic detection. At this point we realized that although this malware had been around for almost a year, we were looking at a hitherto-undocumented commodity RAT.

For Sale

Commodity RATs are typically peddled on underground forums and come and go with new offerings springing up to replace those taken down by law enforcement actions.

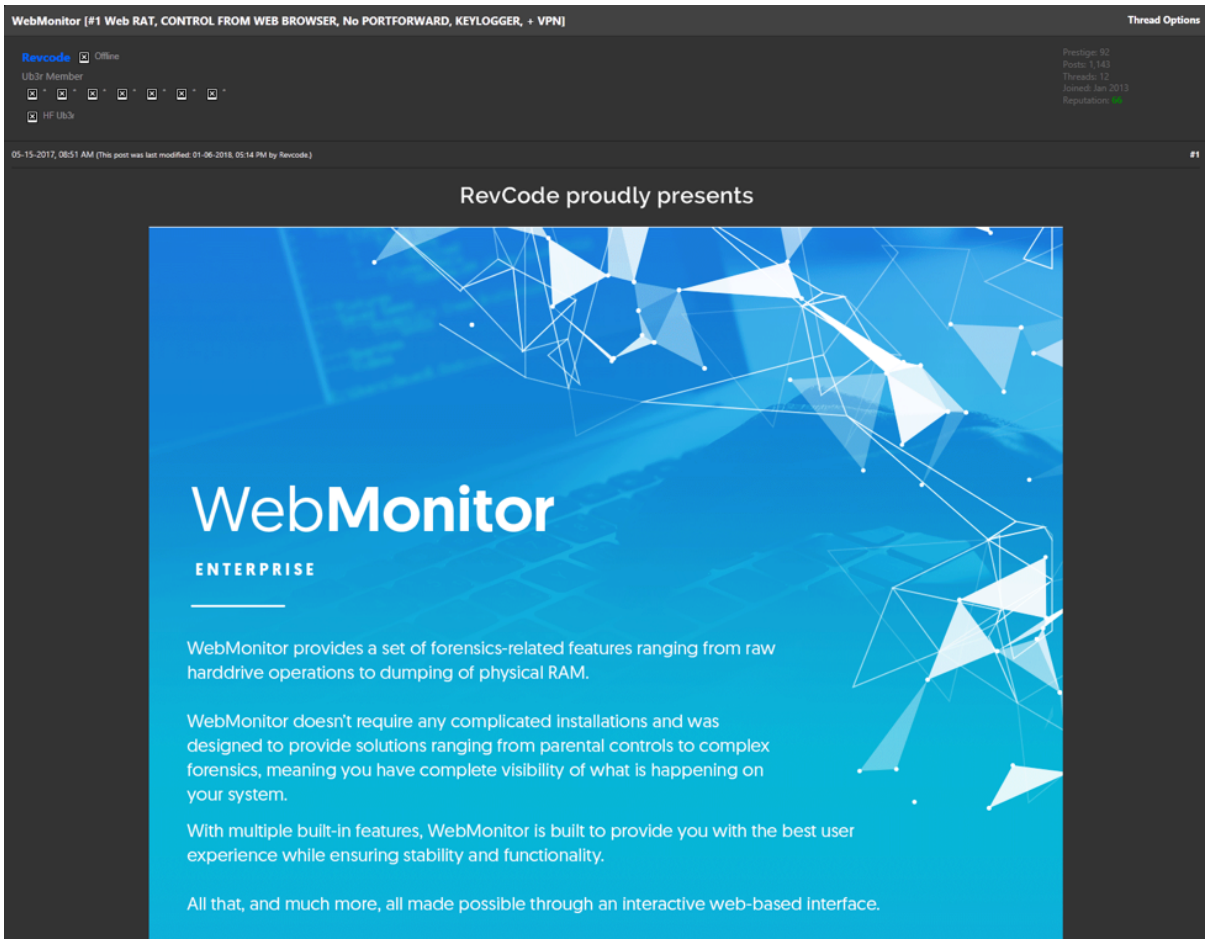


*Figure 1 – WebMonitor RAT Forum sales thread*

We first observed apparent tests of this RAT in late February 2017. In May 2017, “Revcode” advertises his RAT “WebMonitor” at hackforums[.]net (Figure 1) for €14.99 - €29.99 (Figure 2):
“[#1 Web RAT, CONTROL FROM WEB BROWSER, No PORTFORWARD, KEYLOGGER, + VPN]”.


*Figure 2 – Editions of WebMonitor RAT sold at three different pricepoints.*

In addition to forum sales thread, Revcode's main sales and support site is at revcode[.] eu (Figure 3).

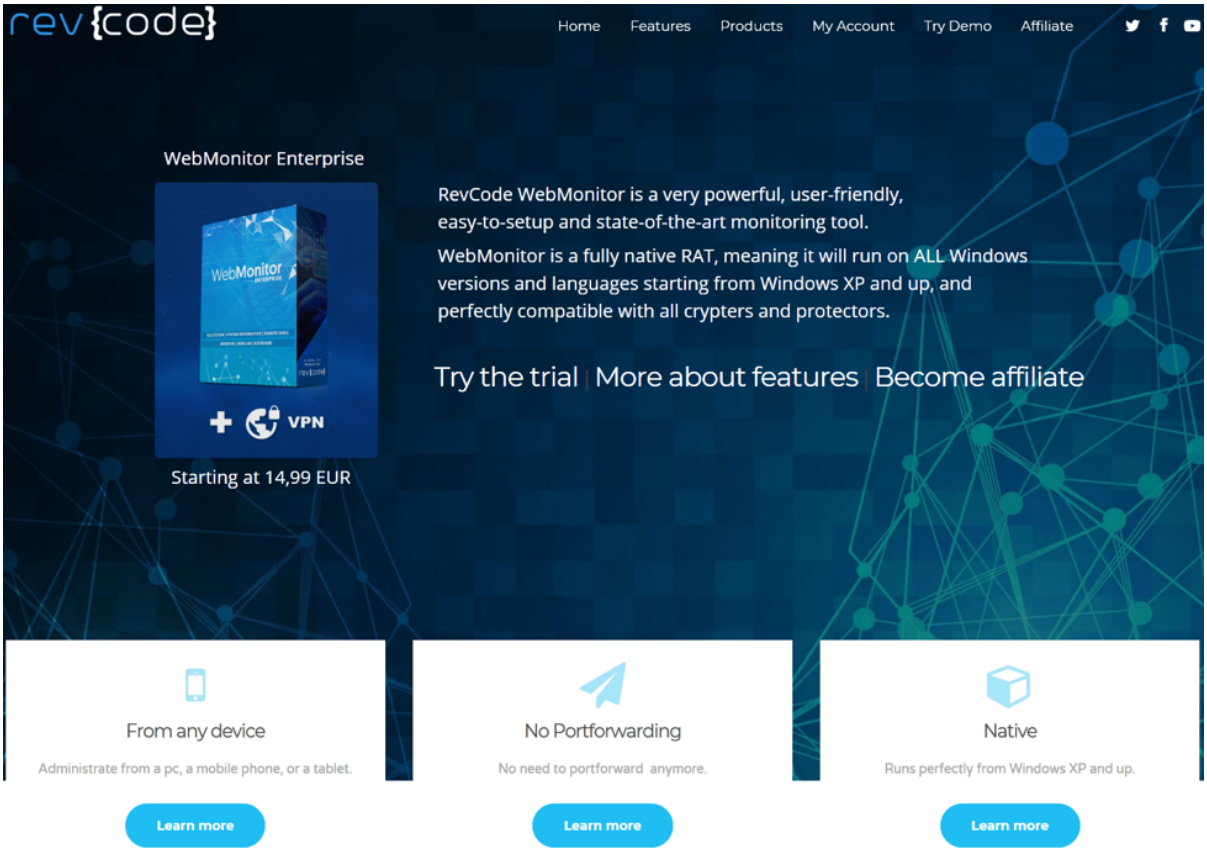


*Figure 3 – Screenshot of revcode[.]eu advertising WebMonitor*

Features

On the server-side, WebMonitor offers an included VPN and C2 service (discussed in detail later in this report), with a web-based interface (Figure 4).

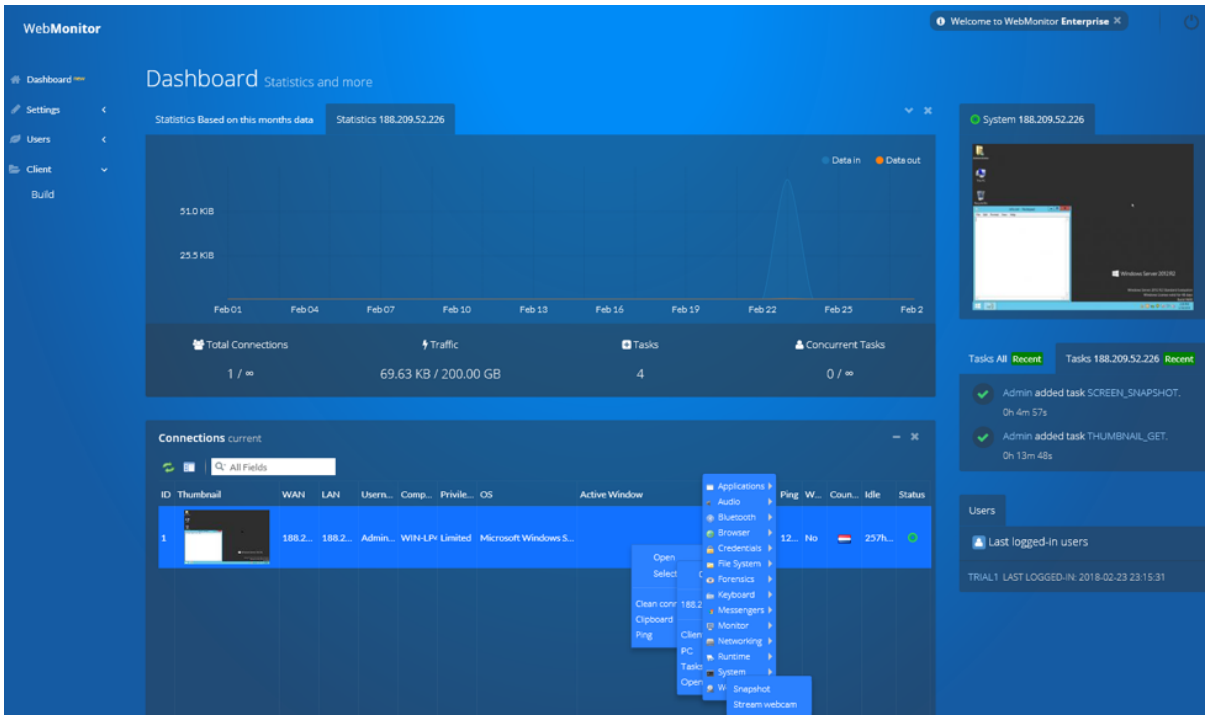


*Figure 4 - Web-based C2 interface*

WebMonitor offers two interface options: the original “Lite” version, and a slicker interface in the “Enterprise” version.

A list of features is provided at the site, some of which stretch the guise of a legitimate administration tool:

- Applications
  - App crash log
  - Injected DLLs list
  - Installed codes list
  - Loaded DLLs list
  - Overview
- Bluetooth
  - Bluetooth log view
  - Bluetooth view
- Browser
  - Addons list
  - History
  - Image cache

- Credentials
  - Browser
    - Passwords
  - Mail
    - All clients
  - Messenger live
    - All clients
  - Network
    - Net pass
    - Wifi key view
  - System
    - Keys
  - Filesystem
    - Disk smart view
    - File browser
    - Recent files list
  - Forensics
    - Harddrive operations
    - Physical RAM dump
  - Keyboard
    - Harddrive operations
    - Physical RAM dump
  - Messengers
    - Harddrive operations
    - Physical RAM dump
  - Monitor
    - Harddrive operations
    - Physical RAM dump
  - Networking
    - Net route view
    - TCP analyze
    - URL protocol view
    - User profiles view
    - WiFi info
    - WiFi channel monitor
    - WiFi history
    - Wireless networks
    - Wireless watcher
  - Runtime
    - Blue screen log
    - Turned on times

- System
  - Battery info
  - Connections
  - Device manager
  - Drivers
  - Firmtables
  - Hardware manager
  - Information
  - Internal activity
  - MUI cache
  - Process manager
  - Remote registry
  - Remote shell
  - Security software list
  - Services
  - Startup view
  - Win logon activity
  - Windows list
  - Windows update list
- Webcam
  - Snapshot
  - Stream Webcam

A recent development, in January Revcode partner “Softpatch” offers an Android RAT client, posting the source code at Github.

WebMonitor Client

The WebMonitor client (ie: the RAT) is written in Visual Basic 6 (VB6) and packed with UPX. It installs to users\%USERNAME%\AppData\Roaming\REVCODE-***.EXE,
where **** is a random 4-digit hex value.
For persistence it creates a registry key under
**x86:** HKCU\Software\Microsoft\Windows\CurrentVersion\Run
**x64:**HKCUU\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run) (Figure 5), similarly appending using the same 4-digit value.

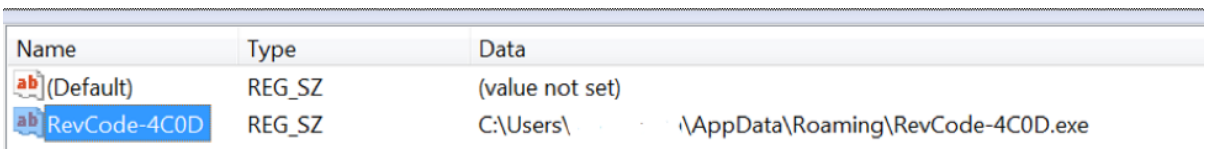

*Figure 5 - Persistence registry key*

Along with the C2-as-a-Service, the client builder is designed for ease of use, with a focus on simplicity. Along with deciding whether a pop-up is displayed – or not – the customer can decide whether the client should run at startup, and if the process should restart if terminated (Figure 6).

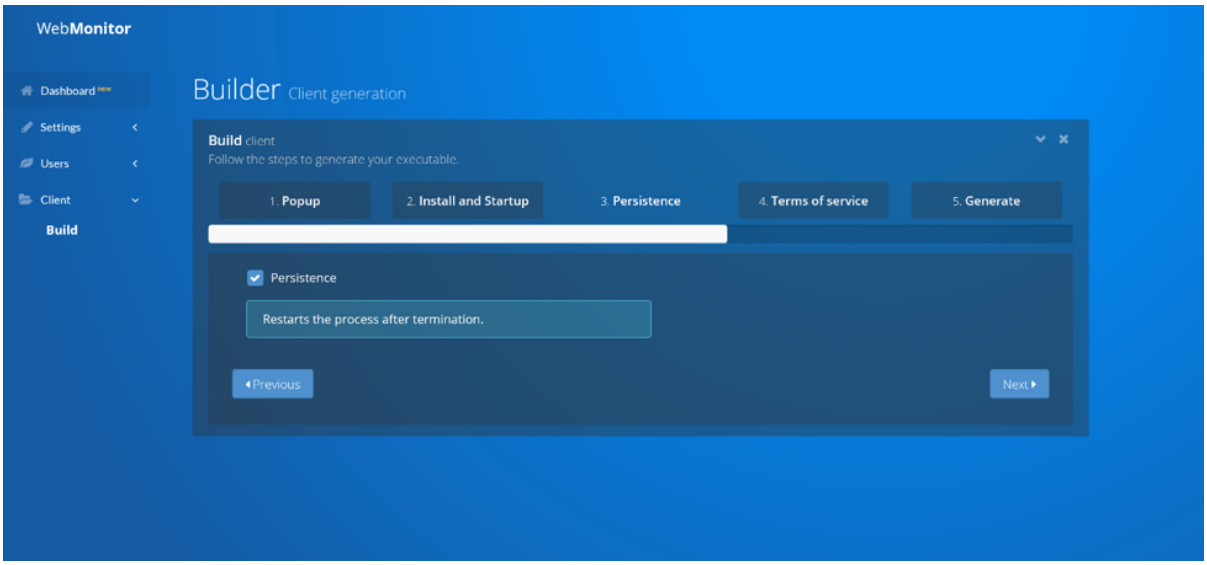


*Figure 6 - Client Builder Interface*

Revcode partner (or alternative forum account) attempts to claim legitimacy "*We have to follow the laws and therefore have to display installation dialogs. However, we can't help if people bypass that by cracking or patching the executable.*" But then contradicts himself in fact, with the builder option to NOT create an installation pop-up, and "*The reason why me made it possible in a way to bypass the dialog is when customers want to update their clients. We don't find it necessary to reproduce the installation dialogs.*".

## C2aaS

As previously seen in Quaverse RAT / QRAT, WebMonitor offers Command-and-Control (C2)-as-a-Service (C2aas). Customers don't have to (in fact, can't) run their own C2 system, it's provided for them. WebMonitor C2s to virtual-hostnames, apparently unique to each customer, at one of two root C2 domains. Although C2 communication is over HTTPS, an obvious downside to such a C2 domain architecture is that the C2 traffic is easily detected and blocked based upon the domains.

WebMonitor customers access their C2 web interface via user-specific virtual hostnames at the host C2s (Figure 7).

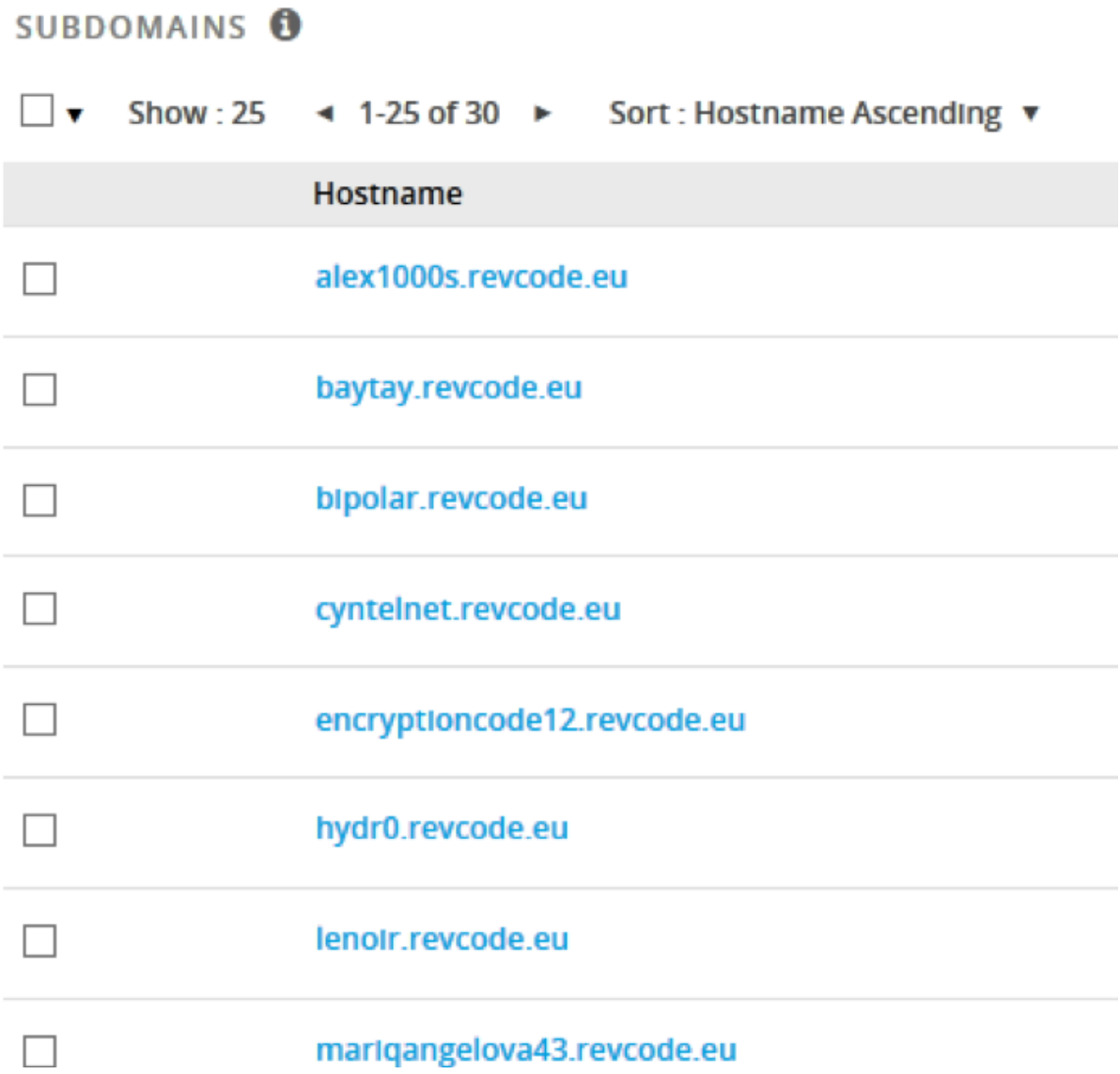


*Figure 7 - C2 Virtual Hosts*

The original C2 domain was the same as the sales website, revcode[.]eu. In late July 2017, a second root-C2 was brought online, wm01[.]to (“WebMonitor”).

DNS & Coin Mining

Starting in samples first observed late-November 2017, in addition to DNS lookups for the C2 as described above, the RAT clients also performed multiple lookups for non-existent domains (Figure 8).

| Query | Response | Type |
|---|---|---|
| wm01.to | ns8-l2.nic.ru | NS |
| pool.minexmr.com | 37.59.43.131 | A |
| sweezzle.53fb0701.to | | NXDOMAIN |
| sweezzle.1e517001.to | | NXDOMAIN |
| sweezzle.93319601.to | | NXDOMAIN |
| sweezzle.efe87401.to | | NXDOMAIN |
| sweezzle.cf488101.to | | NXDOMAIN |
| sweezzle.6a0fe901.to | | NXDOMAIN |
| sweezzle.81252b01.to | | NXDOMAIN |
| sweezzle.69385701.to | | NXDOMAIN |
| sweezzle.49b56c01.to | | NXDOMAIN |
| sweezzle.wm01.to | 185.11.146.81 | A |
| sweezzle.bb8c4e01.to | | NXDOMAIN |
| minexmr.com | ines.ns.cloudflare.com | NS |

*Figure 8 - NXD and Monero Mining Pool DNS lookups*

These take the form <username>.<8_char_hex_value>.to. No domains in any observed samples using this technique actually exist, and as such the DNS “NXD” (non-existent domain) response has no obvious C2 function.
It is possible that this is may be a yet-to-be-implemented Domain Generation Algorithm (DGA) implementation, otherwise possibly a clumsy and ineffectual effort to attempt to camouflage the genuine C2 DNS lookup among invalid ones.
One of the very first samples observed using this new technique also contacted a Monero Mining Pool server pool1.minexmr[.]com, as seen in Figure 8 above. This may have been the

author testing rather than a feature released to his customers, as we only observed this once in the wild. Monero mining is hardly representative of a feature of a “legitimate remote administration utility”.

RAT Customers and Targets

Revcode[.]eu is observed being used less often in recent months, in favor of wm01[.]to, with some samples contacting both. At time of writing, we understand those to be the only two domains used by WebMonitor’s C2-as-a-Service. Based upon analysis of passive DNS records, we observed just under 100 virtual hosts under the two domains, giving an indication of the relatively small number of customers. To date Palo Alto Networks has collected just over 500 distinct samples of WebMonitor.

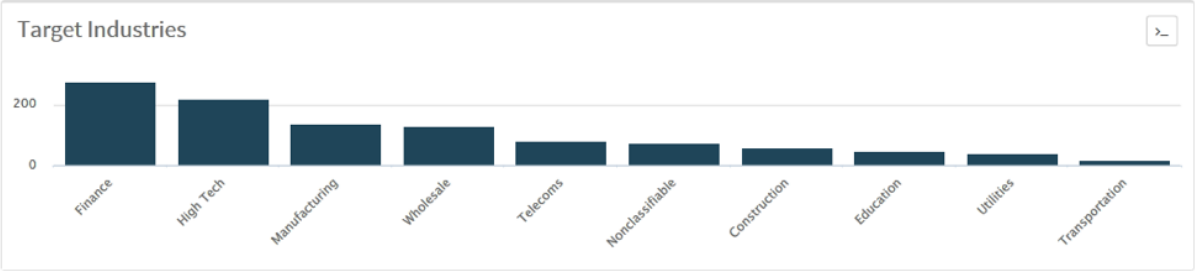


*Figure 9 - Verticals*

The apparently-small number of customers and the “commodity” nature of this malware, with a modest price tag, might suggest an innocuous threat. However, using AutoFocus, we have observed over 2000 WebMonitor infection attempts against Palo Alto Networks customers across multiple verticals (Figure 9), worldwide (Figure 10).

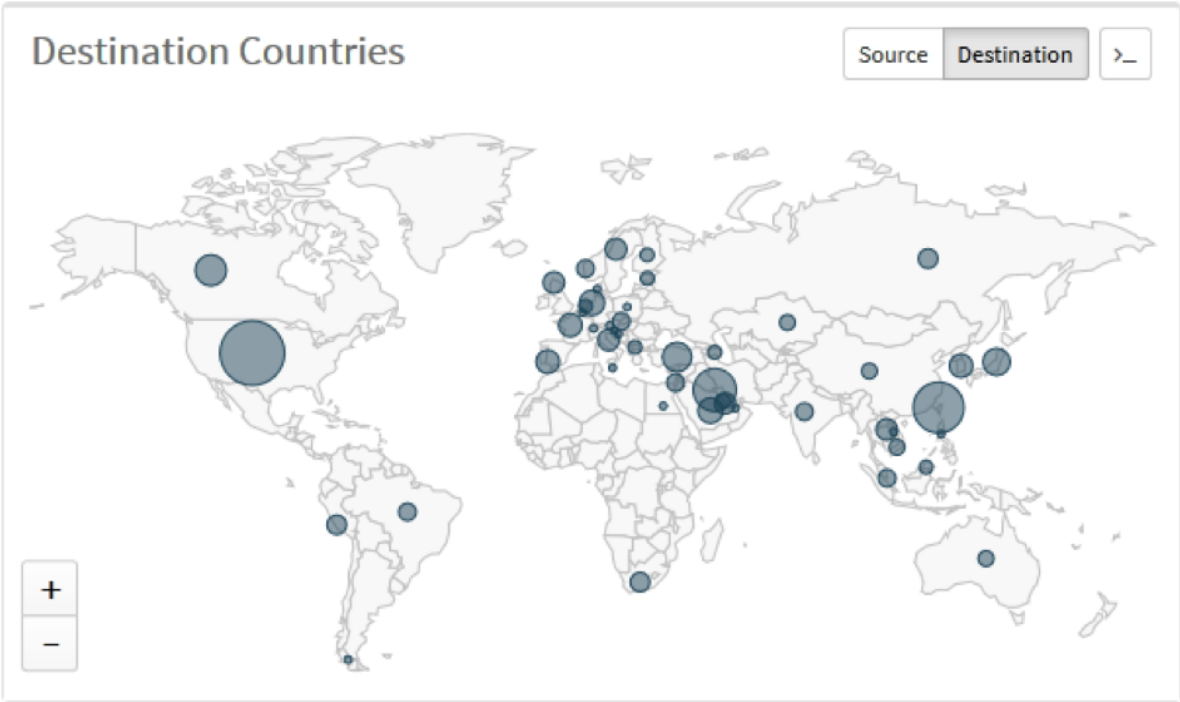


*Figure 10 - Global distribution of targets*

Author

The domain revcode[.]eu has an in-the-clear, non-anonymized WHOIS (Figure 11). Several current and historical domains are registered with identical information, some back to 2013. Research into the information in the WHOIS found corroborating information, identifying a 25-year-old from the state of Bavaria in southern Germany.

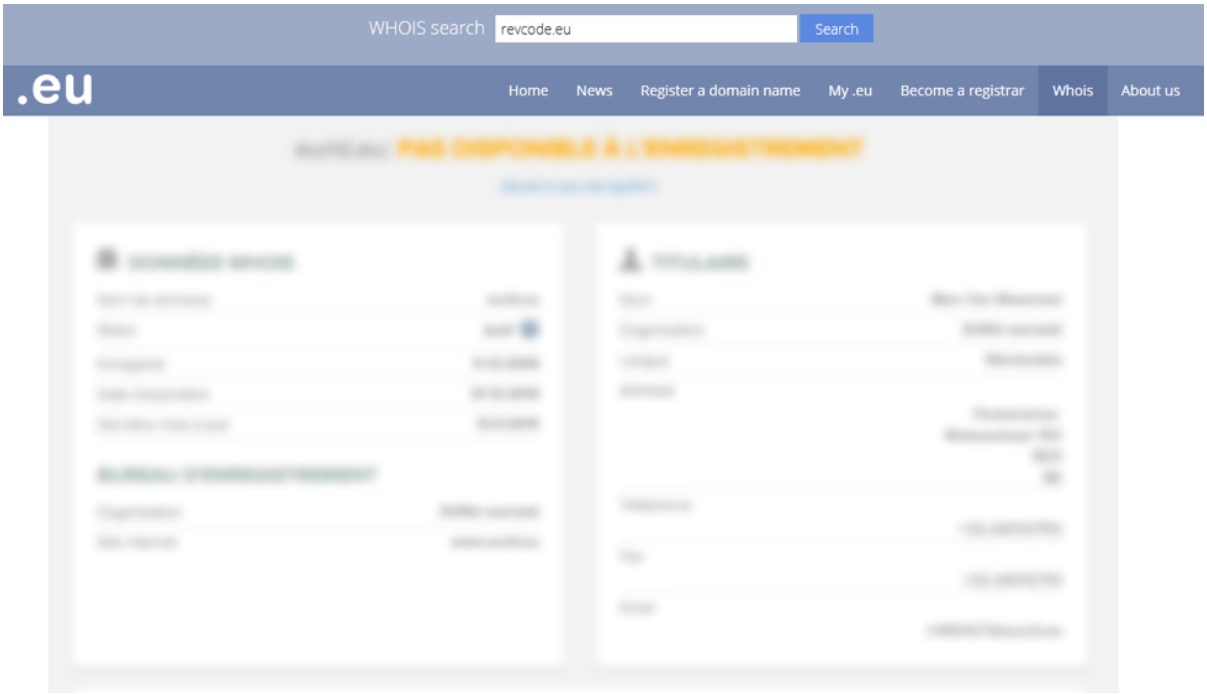

*Figure 11 – en-clar revcoce[.]eu WHOIS registration*

Interestingly, while WebMonitor has been marketed since May 2017, there has been no other formal analysis and write-up in the year that it has been sold. The tongue-in-cheek, Florida-based blogger “Krabs on Security” offers an analysis, but this hasn’t been picked up by mainstream malware researchers. She opines “*a very very legal malware backed by a .eu domain and a very very long Term of Service that was used in CEO Fraud, as seen below. Who would’ve thought such legal software being advertised on the benign forums dubbed “HackForums” would be used for such notorious cybercriminal purposes?*”. “Revcode” partner “SoftPatch” seemed slighted and was quick to attack this analysis, pointing out in a forum post (Figure 12) multiple apparent inaccuracies.

I believe the link you've provided refers to k rabsonsecurity .com. Observe: "KRABS", not "KREBS". There is also a reason why HF has censured that domain, but that's a different story.

k rabsonsecurity .com is simply a new, wanna-be, with absolutely no credibility (at least according to alexa.com) and has absolutely no statistics what so ever.
To us, that article (not to mention the whole website) is just nothing more than a fraud itself. It's not referring to any sources, making it pretty obvious that it's operated by some/someone lacking necessary academic background.

However, I'll admit that some of the analysis made in that article of the WebMonitor executable are somewhat accurate, but limited to a fraction.
Their "reverse engineering" of the WebMonitor executable is far from proper. A typical sign of a rookie reverse engineer.

Based on the "analysis" in the article, a .NET de-compiler is being used, de4dot. Really?
Someone has clearly not realized that it's meant for unpacking/de-obfuscating .NET applications, and not native VB6 apps. There is a difference between those two, so that's some stupidity right there to start off with.
Any experienced reverse engineer would've used completely different reversing approach and tools.
k rabsonsecurity .com further fails to realize that the .NET "like" code generated as result from the .NET decompiler used for this "analysis" is actually converted native code into .NET code, making them believe it's actually coded in .NET.

Anyway, let's dig into a few things that makes those lazy "researchers" garbage instead:

1. Article suggests WebMonitor P2P-based. A P2P RAT? What, really? Revcode has never suggested anything like that. Anyway, next.

2. Article suggests that byte_ = Convert.FromBase64String(s); is the decryption routine of the settings. Wrong! A second layer is missing here after base64, AES.
For traffic encryption, we are using a proper LZW plus AES128 encryption with a keys being exchanged using a Diffie-Hellman based handshake protocol as top layer. (see sources)
Most other paid RATs don't even have that, but rather hard-code the encryption keys with the binaries. It's not my objective to identify those with this post.

3. Article talks about RevCode not knowing what encrypting strings in a binary is. Revcode flips the question and ask why should strings be encrypted in a binary in the first place when they will be decrypted in memory anyway? And how would that be decrypted? Simply by reading a hard-coded encryption key from the binary itself. What's the point?
Article author hasn't realized that the use of hard-coded encryption keys completely contradicts the purpose cryptography.
By that said, we simply find no point in encrypting strings in the binary. Crypters, anti-cracking tools and exe protectors can simply deal with that instead.

4. Article suggests Revcode claims WebMonitor to be coded in C++, simply based on a random HF member's post in the sales thread. Really?
Revcode has never claimed it to be coded in C++. However, some plugins used with WebMonitor are coded in C++, for example the webcam plugin, which is based on DirectShow (DirectX). (see source).

5. Article argues about the startup method used with WebMonitor. Once again, crypters, anti-cracking tools and exe protections can easily deal with that if needed.

6. The article further mentions the password recovery method used with WebMonitor, specifically suggesting it's using NirSoft. Hey, what happened to the "reverse-engineering"?
Can admit we used a list from NirSoft as they have neatly organized all latest browsers and their versions. Secondly, article author must have forgot that it's not possible to use NirSoft anymore ever since they removed command-line based recovery tools for browser passwords a while back ago.
So how are we doing it? (see sources)

7. The article further argues that the RAM Dumping method used with WebMonitor "will surely not be used for POS fraud".
Even worse, they compare it to a RAM Scraper, which is something completely different.
Now this is what I believe; First of all, author has most probably no idea what he's talking about. RAM Scraper actively monitors RAM for targeted data. WebMonitor's RAM Dumper doesn't do that.
The RAM Dumping method used with WebMonitor takes a snapshot of the physical RAM and dumps it to the hard drive. The process can take up to several minutes depending on the capacity of the RAM. Realistic chances of any sensible, not to mention plain (non-encrypted), POS data being stored at that very moment are almost non-existent. Article author probably mixed RAM Dumping up with TCP Dumping/sniffing, which is something completely else, but at least more relevant.

8. Reading the associated comments to the article just confirms that the "researcher" seriously lacks reversing skills when suggesting that NirSoft tools are coded in .NET.
As far as I know, NirSoft recovery tools are coded in C++. Want to check it up? Have a look at their executables with PEiD for example.

9. Article suggests that WebMonitor "has .NET dependencies in some modules". I'd personally really like to know how a native VB6 app can have .NET dependencies for some modules.
That's something just impossible. Further, msvbm60.dll is not a signature provided by Revcode. I'm not even going to bother explaining what msvbm60.dll is, but letting Google deal with that instead for anyone interested. However, that's something one gets wrong when not knowing how to reverse engineer properly.

10. Finally, article suggest it's a copy pasted app. The handshake protocol itself should be sufficient enough to prove the opposite, which can't be found anywhere else as it was converted by me from C++.
Anyone challenging that can feel free to PM me for more unique codes.

Sources:
Handshake protocol: https://imgur.com/a/6bVv9
AES enc snippet from cAES.cls: https://imgur.com/a/Slc8J
Password recovery: https://github.com/AlessandroZ/LaZagne
WebCam plugin: https://github.com/tedburke/CommandCam

Finally, we almost certainly know which HF member is operating k rabsonsecurity .com, but we are not to talk about that in this thread, but what I can say though is that one of its main objectives is harm targeted paid RATs on the market, and nothing else.

*Figure 12 - SoftPatch fires back at krabsonsecurity*

And Revcode himself, despite the usual attempts at pretense-of-legitimacy seen in Commodity RAT sales, markets features that have no utility for legitimate use: “*perfectly compatible with all crypters and protectors*”, “*Privacy is our priority, so no logs are saved on our servers.*”. Revcode partner (or alternative forum account” posts an exhaustive list of

credentials that this RAT can recover "*Here is a list of what kind of credentials RevCode is capable of recovering*":

***Web Browsers:***

** Internet Explorer 4.0 - 11.0*
** Mozilla Firefox - All versions*
** Google Chrome*
** Safari*
** Opera*

***IM Clients:***

** MSN Messenger*
** Windows Messenger (In Windows XP)*
** Windows Live Messenger (In Windows XP/Vista/7)*
** Yahoo Messenger (Versions 5.x and 6.x)*
** Google Talk*
** ICQ Lite 4.x/5.x/2003*
** AOL Instant Messenger v4.6 or below, AIM 6.x, and AIM Pro*
** Trillian*
** Trillian Astra*
** Miranda*
** GAIM/Pidgin*
** MySpace IM*
** PaltalkScene*
** Digsby*

***Email Clients:***

** Outlook Express*
** Microsoft Outlook 2002/2003/2007/2010/2013/2016*
** Windows Mail*
** Windows Live Mail*
** IncrediMail*
** Eudora*
** Netscape 6.x/7.x (If the password is not encrypted with master password)*
** Mozilla Thunderbird (If the password is not encrypted with master password)*
** Group Mail Free*
** Yahoo! Mail - If the password is saved in Yahoo! Messenger application*
** Hotmail/MSN mail - If the password is saved in MSN/Windows/Live Messenger application*
** Gmail - If the password is saved by Gmail Notifier application, Google Desktop, or by Google Talk*

***Windows Network Credentials:***

** Login passwords of remote computers on your LAN*

** Passwords of mail accounts on exchange server (stored by Microsoft Outlook)*
** Password of MSN Messenger / Windows Messenger accounts*
** Internet Explorer 7.x and 8.x*
** The passwords stored by Remote Desktop 6*

***Protected Storage:***
** Outlook 97*
** Outlook 2000*
** Outlook XP, 2003, 2007, 2010, 2013, 2016*

***Product Keys:***
** Microsoft Windows XP, Vista, Server, 7, 8, 10*
** Microsoft Office 2000, 2003, 2007, 2010*
** Microsoft SQL Server 2000, 2005*
** Microsoft Exchange Server 2000, 2003*
** Visual Studio*
** Some of the Adobe and Autodesk products*

***Network Credentials:***
** WiFi stored WEP and WPA keys*
** Remote Desktop credentials*

Summary

The feature set of this RAT would afford an attacker significant access to and control of a victim. Fortunately, owing to the "C2aaS" model employed, detection of and prevention against WebMonitor C2 traffic is trivial. Webmonitor's addition to the list of currently-marketed commodity RATs demonstrates their continued popularity, enabling successful attacks even in the hands of the unsophisticated attacker.

We predict that WebMonitor won't last much longer, at least not with this model as the C2s are too easily identified/blocked. Indeed, another aspect of this centralized model, having the hosted service create each client for customers, might put the author's hands on every one of the malware samples in the eyes of the law.

Coverage

Palo Alto Networks customers are protected from this threat in the following ways:

1. WildFire accurately identifies WebMonitor RAT samples as malicious.
2. Traps prevents this threat on endpoints, based upon WildFire prevention.
3. WebMonitor root C2 domains are flagged as malicious in Threat Prevention.

AutoFocus users can view WebMonitor RAT samples using the "WebMonitorRAT" tag.

IOCs can be found in the appendices of this report.

Appendices - IOCs

**Appendix I – C2 domains**
revcode[.]eu
wm01[.]to

**Appendix II – Sample hashes**
Hashes of WebMonitor samples can be found here.