Imminent Monitor – a RAT Down Under

unit42.paloaltonetworks.com/imminent-monitor-a-rat-down-under

December 2, 2019

By Unit 42

December 2, 2019 at 6:00 AM

Category: Malware, Unit 42

Tags: Cybercrime, Imminent Monitor, Orcus RAT, RAT, Remote Access Tools

This post is also available in: 日本語 (Japanese)

Overview

The availability of "commodity malware" – malware offered for sale – empowers a large population of criminals, who make up for their lack of technical sophistication with an abundance of malicious intent.

Rather than looking just at the malware samples and functionality themselves, we've taken an interest in the commodity malware ecosystem; especially into the malware authors who fundamentally empower and profit from it.

Our previous research into commodity Remote Access Tools (RATs) has assisted law enforcement efforts in prosecuting the authors and customers of malware including Orcus, LuminosityLink and Adwind. Our "SilverTerrier" research into the immensely prevalent West-African financial cybercrime has shown the tremendous popularity of commodity malware empowering the largest financial cybercrime threat at this time, and especially their evolution towards using commodity RATs in their attacks.

One example is of the actors behind the Orcus RAT, which are the subject of recent and ongoing legal action in Canada. This case continues to be prosecuted with vigor. Palo Alto Networks has collected more than 16,000 distinct samples of Orcus RAT since April 2016 through to publishing, and we have observed more than 46,000 unique attacks using this RAT against Palo Alto Networks customers.

We next focused on "Imminent Monitor," a RAT offered for sale since 2012. In comparison to Orcus RAT, we have more than 65,000 samples of Imminent Monitor, and observed its use in more than 115,000 unique attacks against Palo Alto Networks customers. This total number of *samples* includes those shared between antivirus vendors, not just those directly detected by Palo Alto Networks customers. However, the observed *attacks* figure only reflects actual, in-the-wild samples from Palo Alto Networks customers. In most cases, repeated attacks using the same samples and/or blocked by signature detection will not be reflected in this figure, and so the actual total number of attack attempts will be much higher than reflected in this metric. With such prevalence, we had to wonder why the author of this malware has been allowed to continue to profit from this for almost seven years, unchecked.

In order to evaluate the potential of success of legal action against a malware author, some of the first questions we ask are who are they, and where are they? This fundamental intelligence will drive the interest and ability of law enforcement to prosecute and inform researchers to which agency they might refer to this case. In the case of Imminent Monitor, Unit 42's referral and subsequent, ongoing cooperation helped initiate and drive international law enforcement action to proceed with charging those responsible for the development and management of this malware, their customers, and the disabling of access to their victims.

Shockwave™'s RAT

In 2012, a developer, "Shockwave™", registered the domain imminentmethods[.]info, and in April 2013 started selling his "Imminent Monitor" RAT on online forums and at his site, which later changed to imminentmethods[.]net. Earlier in 2012, he had offered a Distributed Denial of Service (DDoS) tool, "Shockwave™Booter," but seemed to drop that project in favor of his new RAT.

He proudly claimed "*the fastest remote administration tool ever created using new socket technology that has never been used before.*"

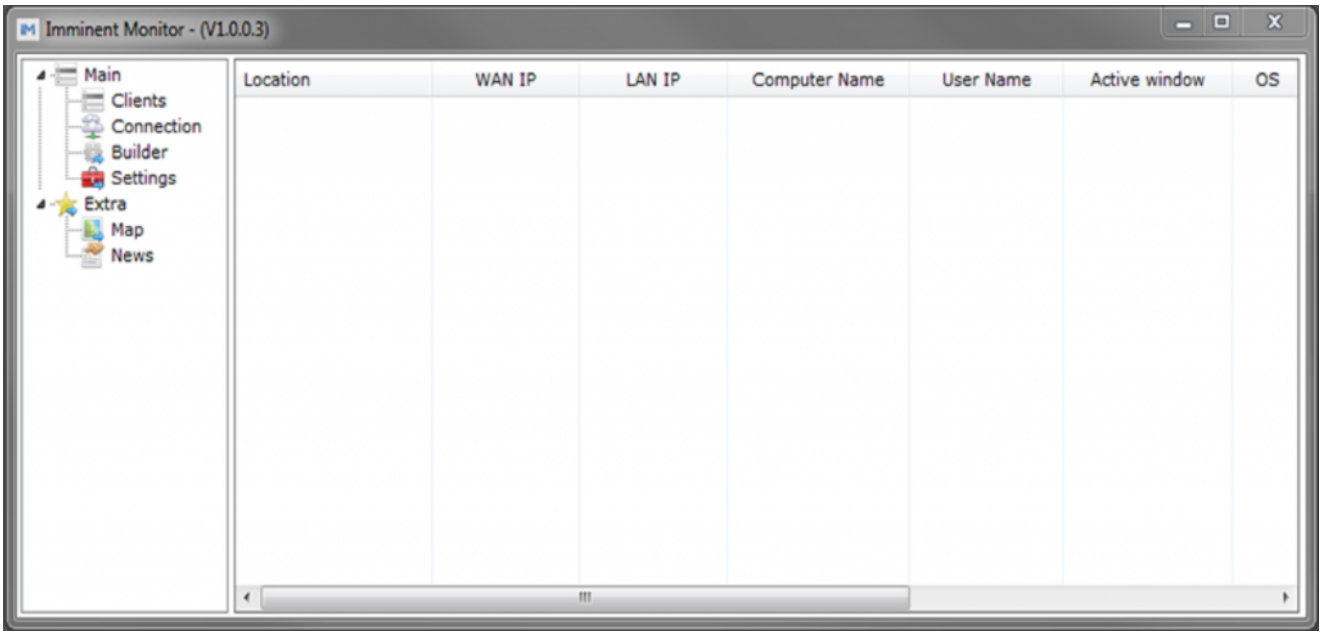

Figure 1. Imminent Monitor 1.0 Client Control Panel

The ImminentMonitor Client Control Panel offers a clean, easy-to-use interface to build (Figure 1) and control (Figure 2) ImminentMonitor client malware. As well as the full Remote Desktop access of any RAT, features less noticeable by the victim include:

- File manager
- Process manager
- Window manager
- Clipboard manager
- Registry manager
- Startup manager
- Command prompt
- TCP connection
- Remote webcam monitoring
- Remote microphone monitoring
- Password recovery

Shockwave™ claimed: "*We use new methods not used in any rat, the remote desktop has the potential to get around 60 fps, and the cam I have personally gotten 130 with this.*"

In 2014, Imminent Monitor started supporting third-party plugins. The first of these offered the ability to turn the webcam light off while monitoring. *Shockwave™ wrote: "Hey, good job on being the first to release a plugin for Imminent Monitor*." – a plugin with an obviously illegitimate intent.

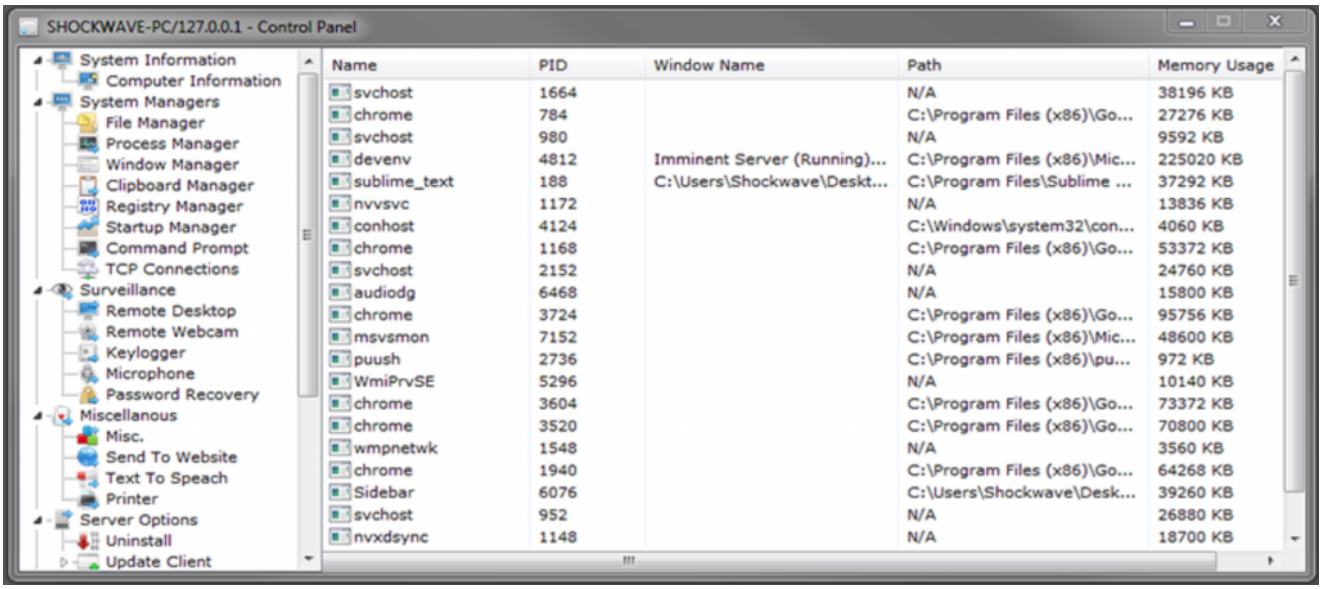

Figure 2. Client control

The features of a(n il)legitimate Remote Access Tool

As very typical with commodity RATs, the authors attempt to profess innocence and distance themselves from the illegitimate features and intent of their malware:

"*We at Imminent Methods are not responsible for the nature in which you use our services. The services sold on this website are for personal, not distributed, use and should only be used on your own machines or the machines of those who have given you expressed consent for remote management. Remember that our tools are made for educational purpose, so we do not take any responsiblity for any damage caused by any of or tools or services. Misuse of our tools or services can be very illegal. Certain misuse could cause possible jail time or fines, which differ depending on your local laws.*" ... "*You agree that you will NOT distribute malicious files created with any of our services over the internet with the intent of harming/using machines of innocent people. You agree that if you do by some sort of means connect to a computer without authorization, by means of accident or other ways, that you will use the uninstall feature to completely remove the connection between the two of you and remove the software from their computer.*" [Sic]

However, Shockwave™'s first-party comments online belie this claim:

"*The keylogger: The logs are hidden, and encrypted, fast transfer of the logs aswell, with progress indicating how much of the log is downloaded*"...
"*The crypter: The crypter is really just a bonus feature, not always FUD but I try and do my best to keep it FUD.*" [Sic]

Legitimate remote access tools don't need to hide and encrypt their logs. A crypter, allowing a "Fully UnDetectable" (FUD) client, only has one purpose: to attempt to evade antivirus detection.

Later versions include “protection” to help avoid detection/removal, also not a feature expected of a legitimate, permissible remote access client (Figure 3).

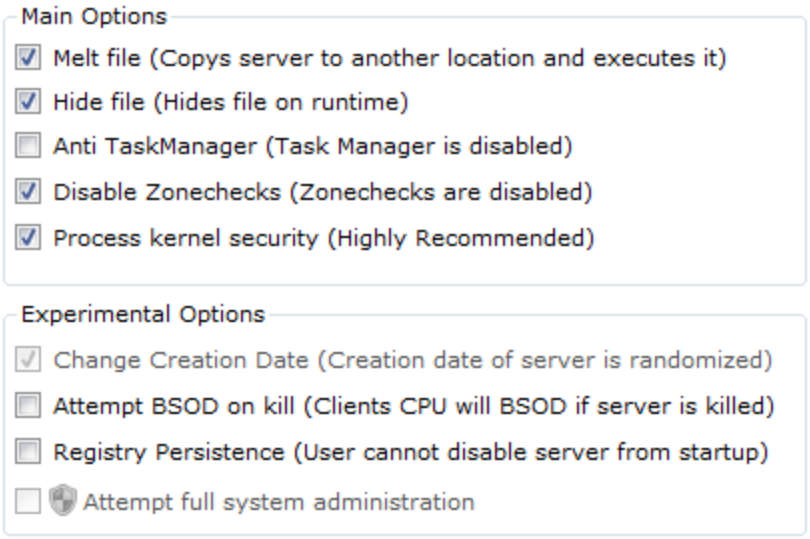

Figure 3. "Protection" features

The most recent sales page for Imminent Monitor continued to profess legitimacy (Figure 4).

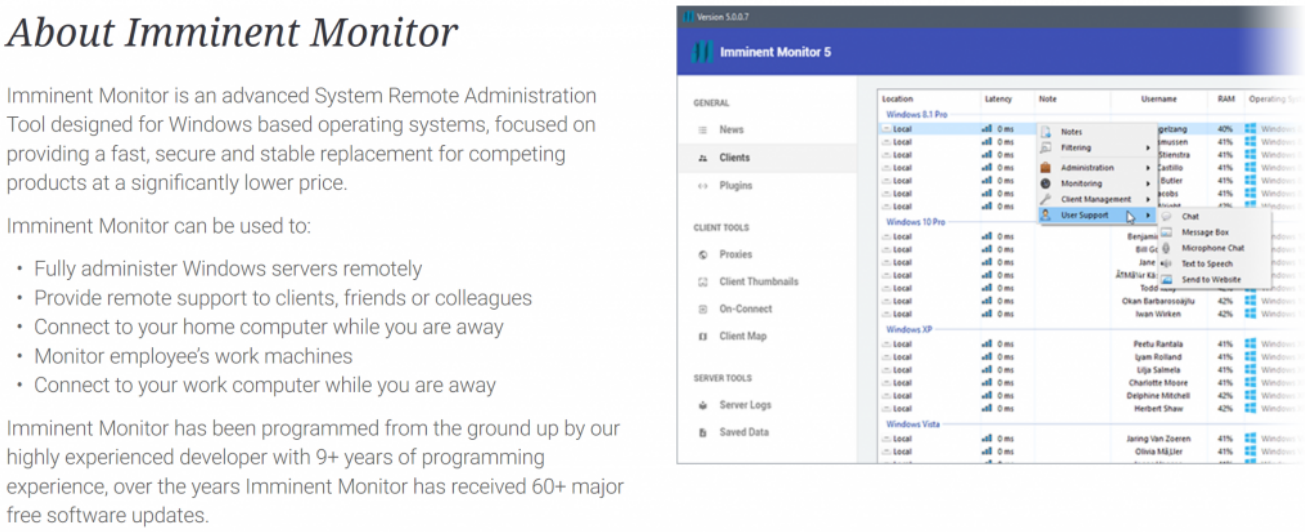

Figure 4. Imminent Monitor "About"

However, features remain that lend utility rather to illegitimate use, hiding the client and maintaining persistence (Figure 5).

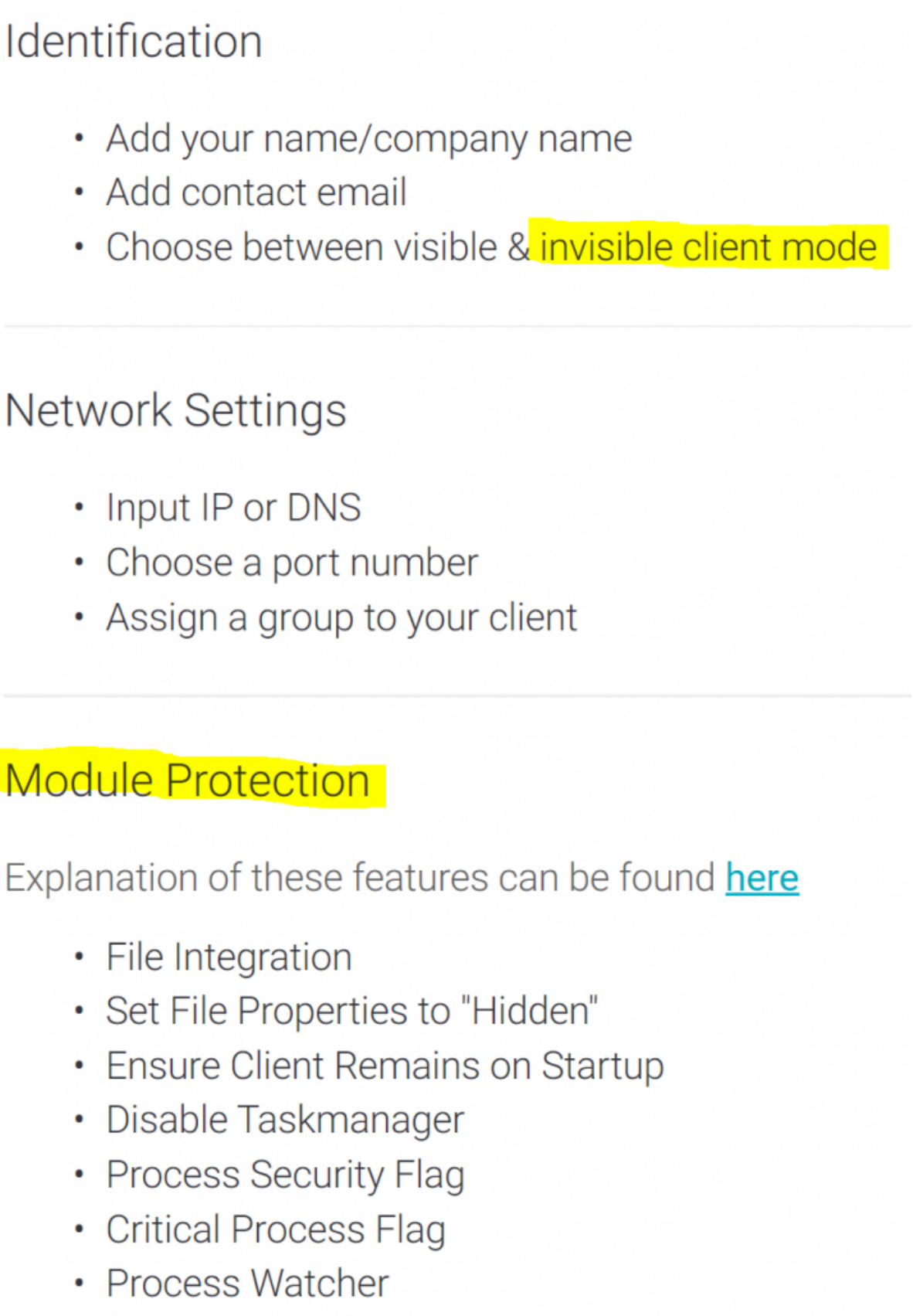

Figure 5. "Protection" features

Shockwave™ promotes the RAT's"protection" features:

"File Integration
The File Integration feature will delete the Imminent Monitor Client from it's execution directory and move it into it's "Client Startup" directory.

Set File Properties to "Hidden"
Does what it says, marks the Client as hidden.

Disable Taskmanager
Disables Windows Task Manager/

Process Security Flag & Critical Process Flag
Both of these functions are currently deprecated as the "Process Watcher" feature replaces them/

Process Watcher
The Process Watcher feature spawns a separate daemon to watch the main Imminent Monitor Client in case the client ever crashes or gets closed."

More recent versions offer what the author terms "HRDP" – *Hidden* Remote Desktop Protocol – offering a non-interactive remote desktop connection, hidden from the victim.

Figure 6. Features

Version 3 of Imminent Monitor introduced the ability to run a cryptocurrency miner on the victim machine – hardly the feature of a legitimate remote access tool (Figure 7).

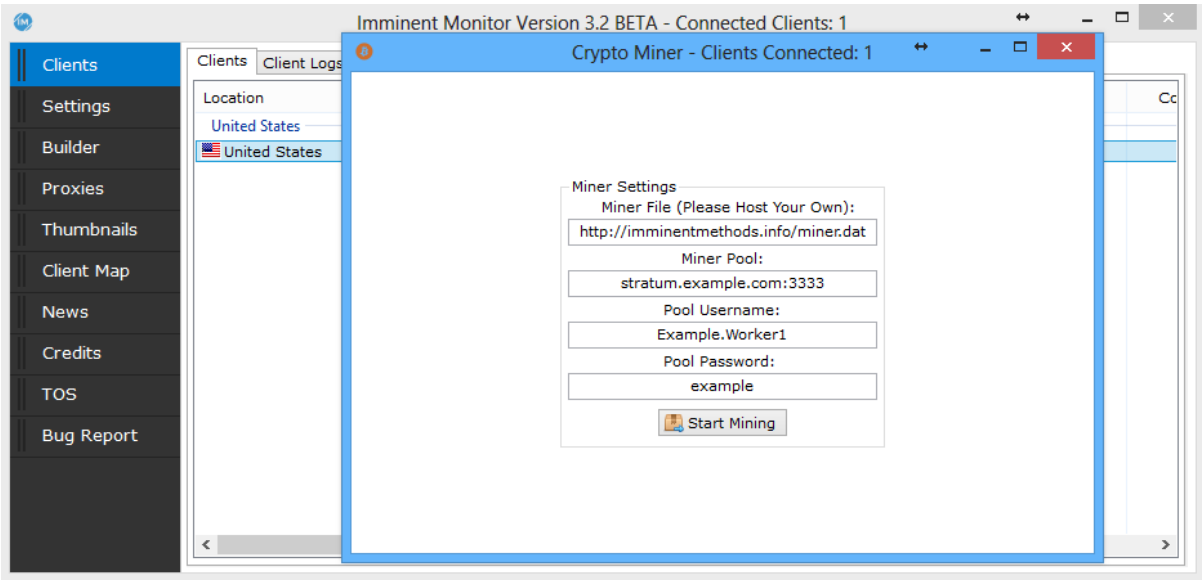

Figure 7. Imminent Monitor Client Cryptocurrency Miner

But, in the end, it will be the courts who will determine legitimacy and intent of the malware author, and also their customers.

Imminent Monitor was originally licensed to each customer for a $25 fee. Six years later, the price has remained static, though new multi-license options are also offered (Figure 8).

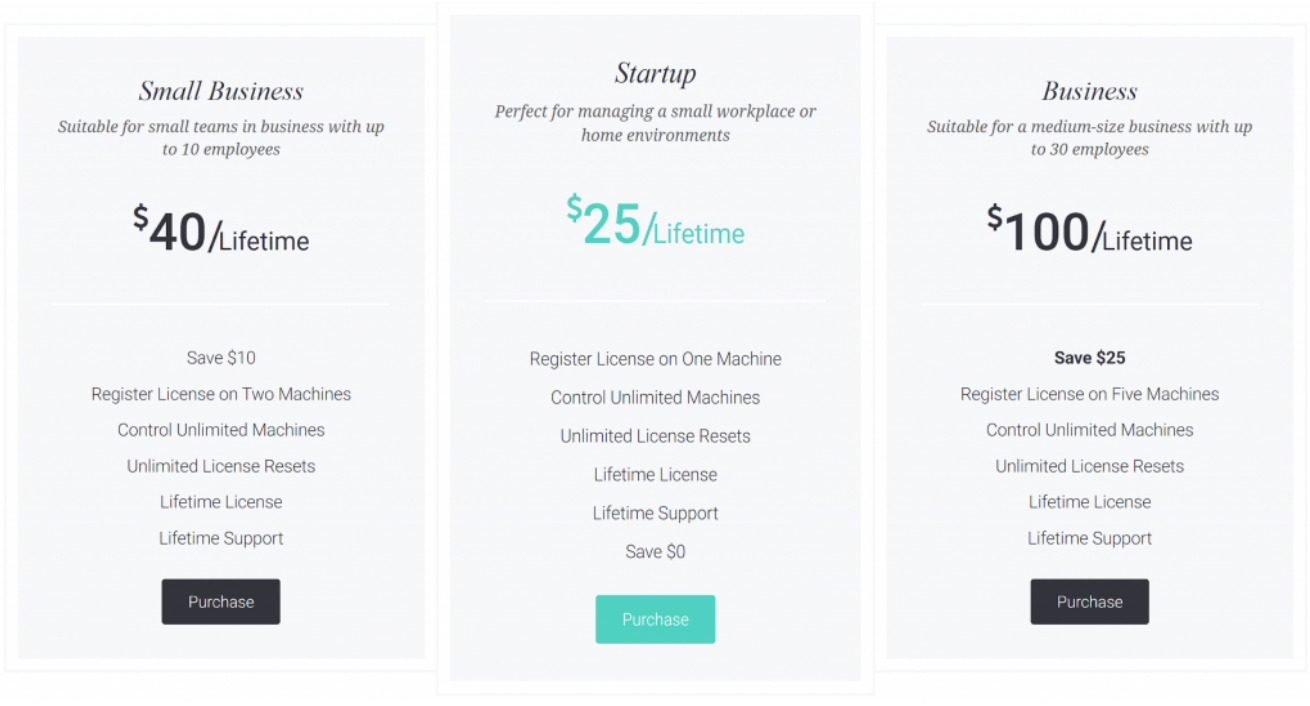

Figure 8. Purchase

Who is Shockwave?

In order to identify actors behind such operations as Imminent Monitor, it's important to be thorough with analysis and intelligence collection. The actor will typically attempt to hide or obfuscate their identity. The research will not only aim to directly identify a specific individual but also help to build a corroborative identity picture, increasing confidence in any analysis.

Infrastructure research did not lead us to any identifying information, though we do notice a definite preference for Australian hosting early on.

Forum profiles for Shockwave™ and Imminentmethods included a common profile photo, a panda-headed business-suited avatar (Figure 9).

Figure 9. Shockwave™/ ImminentMethods' avatar

The Twitter account "imminentmethods" includes a location of "Queensland, Australia". A Google+ account for imminentmethods[at]gmail.com had the same Panda avatar, and the name (redacted here for publication) "J[redacted]".

A deviantart.com profile for user "ViridianX" had the same panda avatar, a link to imminentmethods[.]info, location Australia, and the same name "J[redacted]" again. This handle was corroborated in a forum post:

"*Also, I have noticed I have been getting imitated on various websites lately my only Accounts are:*
shockwave.hf

http://www.twitch.tv/imminentmethods [twitch]
ViridianX [Justin.tv]"

A Paypal purchase from imminentmethods[.]net gave a merchant name "DictumFox"(Figure 10).

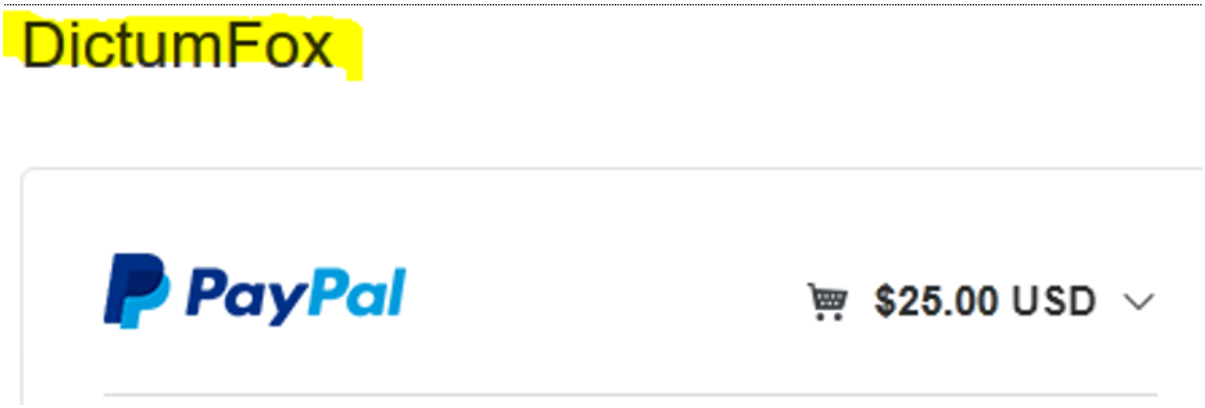

Figure 10. Paypal

This appears to be a unique handle. The site, dictumfox[.]com, previously had the site title "Imminent Methods"(Figure 11).

Figure 11. DictumFox-Imminent Methods

The imminentmethods[.]net "Contact us" page has an Australian phone number and time zone, and a New South Wales, Australia address which comes back to a small-business services address.

A search of the Australian business registry finds a "DictumFox", with a registered agent at the same address of convenience, with a different, female first name J[redacted] K[redacted]. She was also previously linked to another Australian business, "Imminent Methods". That business record has a current agent with the same first name as seen in the profiles - J[redacted] - and the same surname as the female associated with the other business registration: K[redacted].

Further research with name and location corroboration seems to possibly explain the relationship with Shockwave™-J[redacted], and the "J[redacted]" of the corporate registration, beyond the same surname K[redacted] (Figure 12).

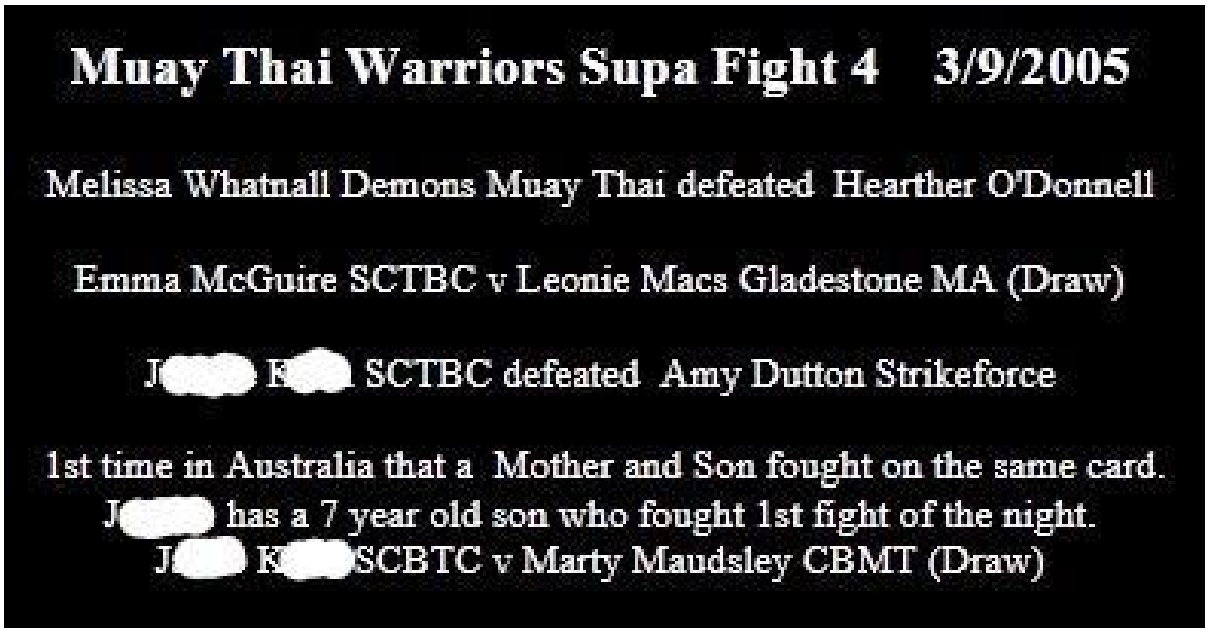

Figure 12. J[redacted] and J[redacted]

Prosecution

Unit 42 referred the identity and activity of Shockwave™ to the Australian Federal Police (AFP) Cybercrime Operations teams. We have subsequently continued to assist the AFP's "Operation Cepheus" (Figure 13), together with the United States Federal Bureau of Investigation (FBI), and Canadian Radio-television and Telecommunications Commission, Electronic Commerce Enforcement / Conseil de la radiodiffusion et des télécommunications canadiennes, Mise en application du commerce électronique (CRTC ECE). The Australian-led investigation, targeting not only those responsible for the development and management of this malware, but also their customers using the malware illicitly, has yielded evidence suggesting in excess of 14,500 customers of this RAT. We most often observe RATs employed illicitly by financially-motivated actors, or for data theft. Interestingly, the AFP's investigation noted a significant number of Australian users of the software were also respondents to Domestic Violence Orders. It's unlikely a coincidence that such a tool might be employed against Intimate Partner Violence victims. AFP's operation also disabled the licensing system of Imminent Monitor, removing users' access to victims of the software. Unit 42's research into the infrastructure and customers of Imminent Monitor and other RATs continues to assist law enforcement internationally in prosecuting the individuals behind such illicit activity, demonstrating the effectiveness and potential of international public/private cooperation in combating cybercrime.

Figure 12. AFP execute an Operation Cepheus search warrant (source: AFP)

Conclusion

We've collected more than 65,000 samples of Imminent Monitor, and seen more than 115,000 attacks against Palo Alto Networks' customers alone. Not only did the availability of this commodity malware enable each of those attacks, the author profited from the sale of it, since 2013.

This Remote Access Tool, promoted first-party on hacking forums, includes features that have no purpose in a legitimate tool but rather are designed to hide attacks using it.

With the successful execution of the AFP's operation, licensed Imminent Monitor builders will no longer be able to produce new client malware nor can the controllers access their victims. Although cracked versions already exist and will continue to circulate, they can't benefit from bug fixes, feature enhancements, support, or efforts to improve their undetectability. Ironically, these versions often carry malicious payloads, acting as infection vectors to the criminals who would use them, themselves.

Organizations with decent spam filtering, proper system administration, and up-to-date Windows hosts have a much lower risk of infection. Palo Alto Networks customers are further protected from this threat. Our threat prevention platform detects Imminent Monitor

malware with Wildfire and Traps. AutoFocus users can track this activity using the ImminentMonitor tag.