The Legend of Adwind: A Commodity RAT Saga in Eight Parts

By Unit 42

Published: 2019-09-17 · Archived: 2026-04-05 16:46:43 UTC

Executive Summary

In early 2012, a developer started selling the first of the Adwind family, Java-based remote access tools (RATs), called “Frutas.” In the ensuing years, it has been rebranded at least seven times. Its other names have included Adwind, UnReCoM, Alien Spy, JSocket, JBifrost, UnknownRat, and JConnectPro.

The Adwind RAT family remains prevalent in the wild. Palo Alto Networks has collected over 45,000 samples from the various Adwind iterations. We have observed these samples used in over 2 million attacks against Palo Alto Networks customers since 2017, highlighting the high impact of this popular commodity RAT.

The first six iterations of the multi-platform Adwind RAT family have been exhaustively documented, so we will not rehash analysis of the RAT itself. This piece describes two hitherto undocumented recent rebrandings: “Unknown RAT” and “jConnect Pro RAT and clarifies some misconceptions. We have identified the author of this commodity malware, demonstrating that ownership of this RAT under its various monikers never actually changed.

This blog post documents Adwind RAT family’s beginning as an alleged science project, evolution to become widely available commodity malware, and eventual refinement into a private sale to what appears to be a closed customer base. By developing a technique to isolate cracked versions from licensed samples, we have documented the impact of the availability of free, cracked versions, and identified researcher reporting as a repeated catalyst to recent rebranding.

A RAT Is Born

On January 11, 2012, Spanish-language indetectables[.]net forum user “adwind” posts about his new “Frutas Rat” project, seen in Figures 1 and 2. A Google translation of the text follows Figure 1.

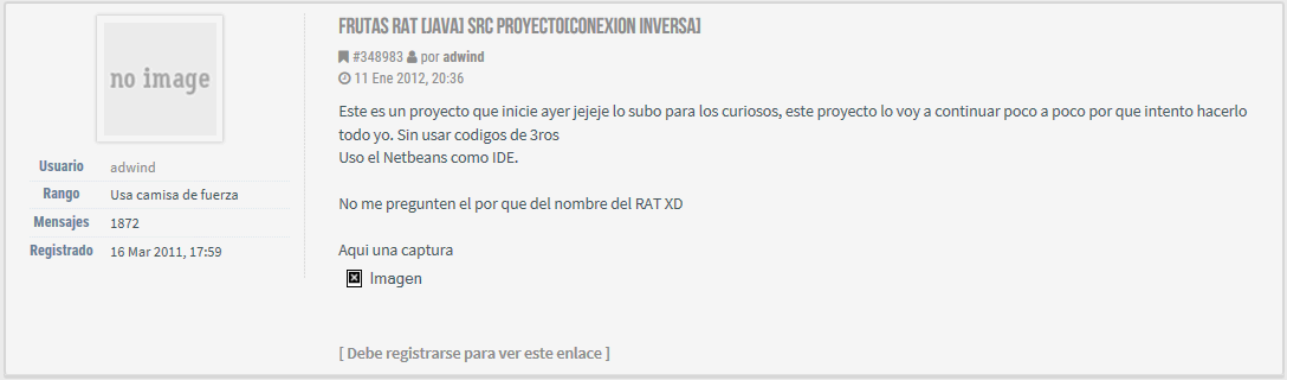

Figure 1. Adwind announces "Frutas"

“Fruits Rat [Java] Src Project [Reverse Connection]…
This is a project that starts yesterday jejeje I upload it for the curious, this project I will continue little by little because I try to do everything myself. Without using 3rd codes
I use Netbeans as an IDE.
Do not ask me why the name of the RAT XD”

Figure 2. Frutas RAT

Through 2012, he released several updates to Frutas. By December 2012, Adwind had rebranded the free Frutas as the paid “Adwind RAT.”

Rebrand

From early 2013, the renamed Adwind RAT was sold at adwind[.]com[.]mx, shown in Figures 3 and 4 below.

PRICE: The current price is $ 55 dollars starting in the February 15 the price is $ 100. DOLLARS
******Contact******
Skype: adwindandres
Email: adwind@gmail.com
Get serial Here!

Figure 3. adwind[.]com[.]mx 2013

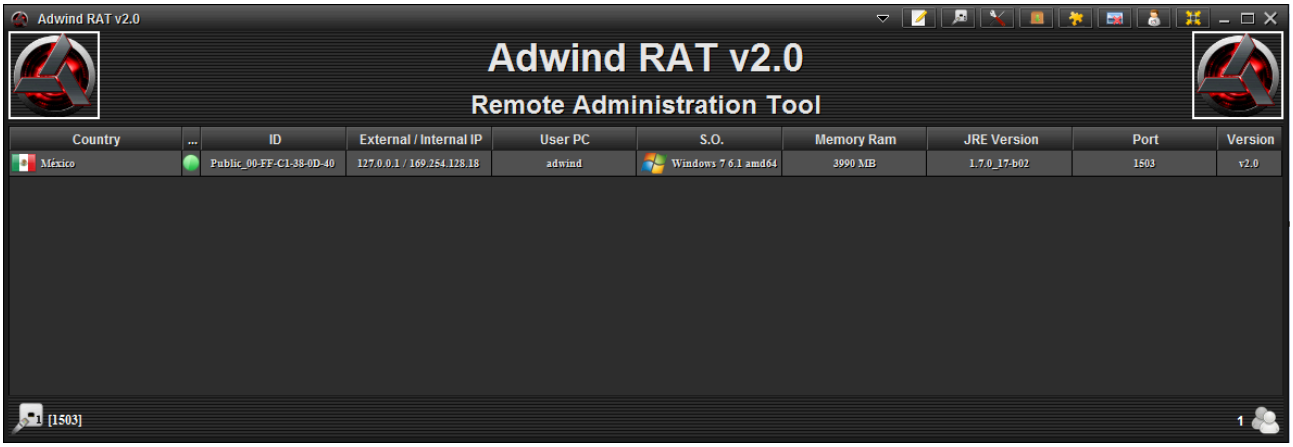

Figure 4. Adwind RAT version 2

On October 5, 2013, Adwind released “V3.0” and claimed that he would be turning the RAT over to “others,” who would also rename the RAT, shown in Figure 5. A Google translation of the text follows the figure.

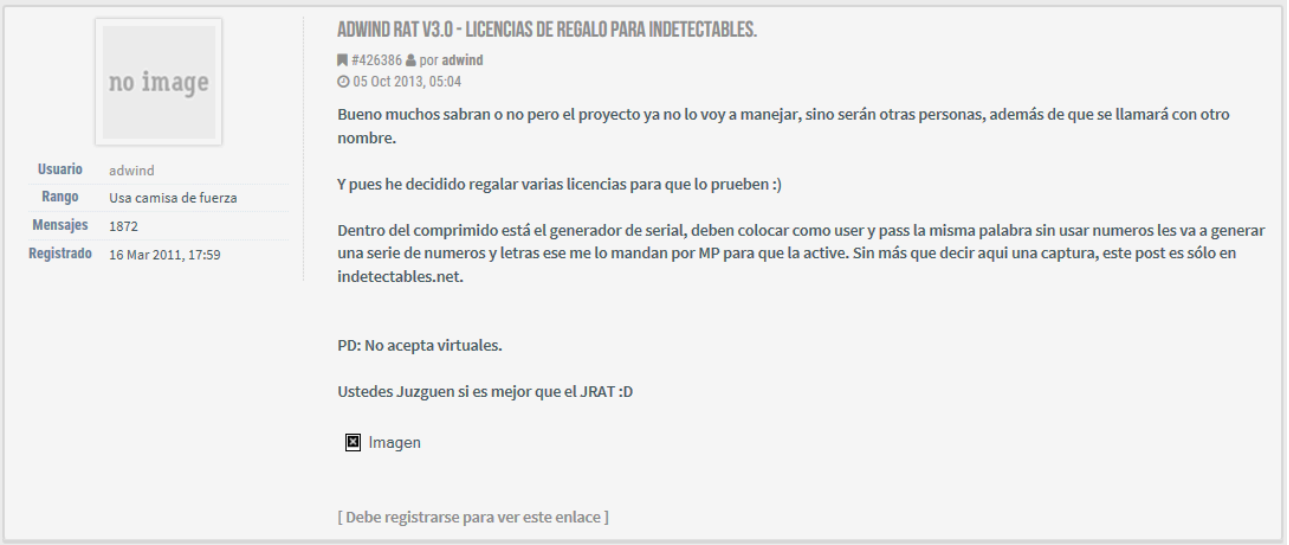

Figure 5. Adwind claims a change of ownership

"Well many know or not but the project already I it will not handle, it will be others that will be called by another name."

Adwind also states:

"You judge if it is better than the JRAT :D"

Some researchers have claimed that JRAT and the Adwind RAT family are related. While JRAT is a Java RAT, we have determined it is completely different and written by a different author.

So, why this rebrand? Although we suspect other reasons for renaming in later iterations of this RAT family, it seems that in this case at least, Adwind's author is specifically trying to distance his identity from continued development and sale of this malware. He may have feared – correctly – that an operational security (OpSec) fail on his part with his Adwind identity might expose his identity and ownership.

UnReCoM RAT

A week after Adwind's "change of ownership" announcement, on October 12, 2013, The domain unrecom[.]net was registered. This site sold the next Adwind family rebrand, "Universal Remote Control Multi Platform" (UnRemCoM) RAT. The ostensible new management is named at the site as "UnReCom Soft" and elsewhere as "Lustrosoft." Figure 6 shows connections to victims in the United States, Spain, and Mexico.

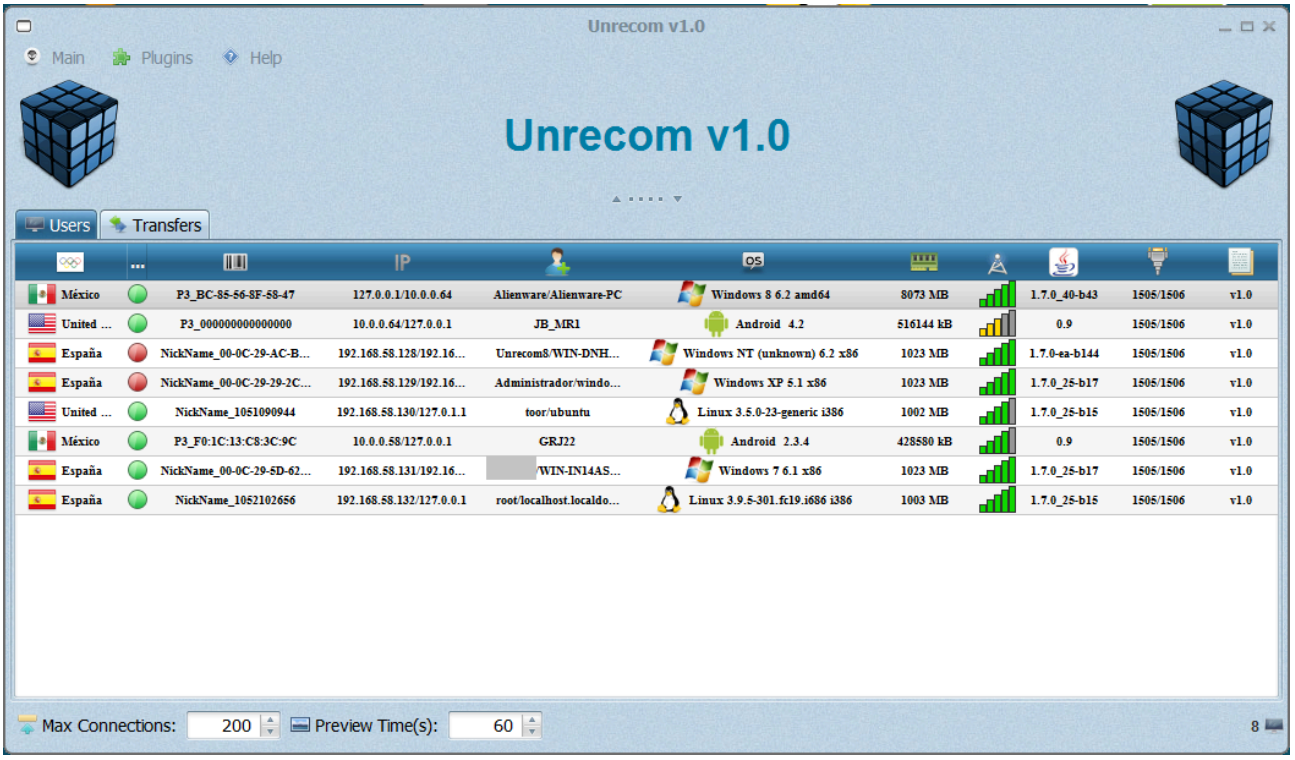

Figure 6. UnReCoM RAT

The site offered a monthly subscription option as well as the ability to purchase the software outright, shown in Figure 7. Some researchers have suggested that this is a “malware as a service” (MaaS) model. However, while commodity malware is often licensed monthly, it isn’t really “as a service” – the user is still wholly responsible for the RAT stub building, C2, “crypting” (stub encryption), and spreading/infection. In contrast, the Webmonitor RAT offered a C2 service that is closer to a MaaS definition.

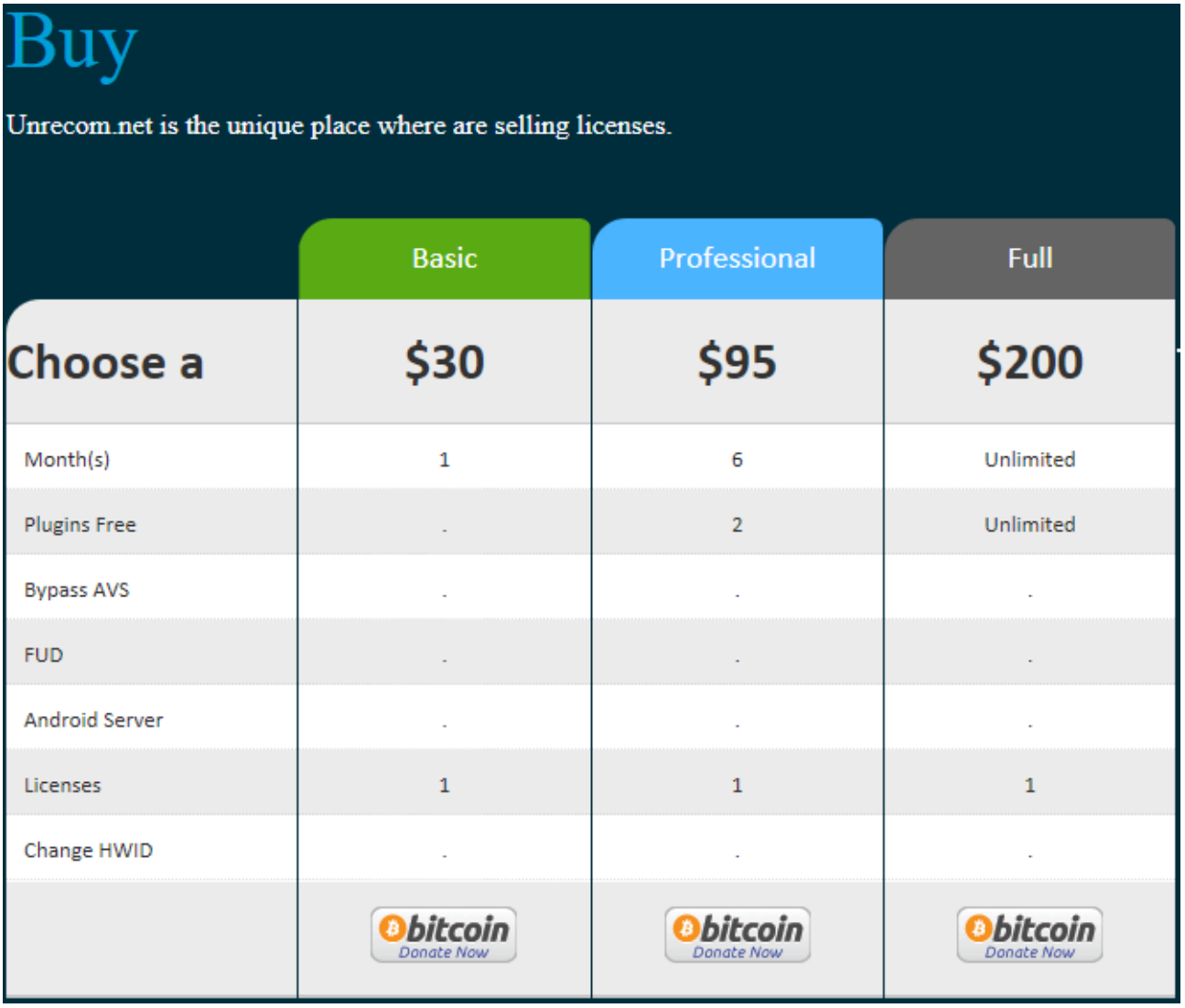

Figure 7. UnReCoM purchase options

The site boasted the multi-platform RAT client availability, listing Windows XP through 8.1, Mac, Linux, and Android:

"UNRECOM is the only software in the world to take control of all operating systems in one place.. You will have full control of your devices in one place."

It also disavowed itself as malware, utilizing bizarre logic:

"Unrecom is a malware?

Not, you need install software in both devices for work."

Alien Spy

Alienspy[.]net was registered June 7, 2014. The reason for this rebrand is unknown. It may be that the author deliberately wanted to circumvent having to honor outstanding purchases/subscriptions and created a "new"

software to be purchased instead. Alternatively, it might be to avoid reputation issues – complaints about various iterations of the Adwind family, lack of support, and dishonoring of purchases are common on forums:

"Alienspy is NO GOOD, it is the worst RAT ever, don't be fooled, the owner needs a lot of money, he cdan make you buy and destroy HWIDS to make you keep purchasing the software, alienspy works sometimes,not all the time, and have an issues with stability, but the owner is very hungry for cash so watch it, he changed the name of several RATs he created and took many people money, do not trust..."

A customer testimonial proudly featured at the site belies any claim of the software's use as a legitimate administration tool, shown in Figure 8 below.

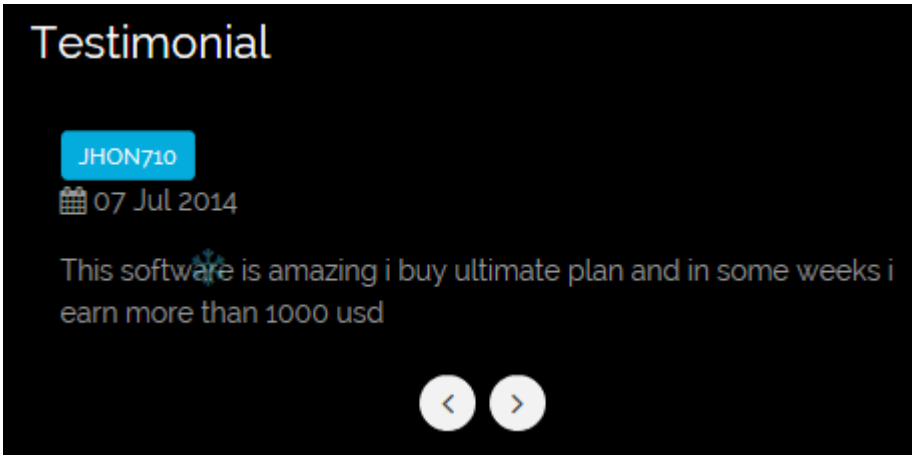

Figure 8. Testimonial

On April 8, 2015, Fidelis released a report on Alien Spy. By the end of April, the domain for the next Adwind family rebrand had been registered, and the registrar had suspended alienspy[.]net. The motivation for this rebrand was quite obvious, although it seems the author didn't lose the opportunity to profit from it:

"i was client of alienspy and bought 1 year member but the rat get suspended before my member expire and when i try to get same discount in the new jsocket i get nothing from the support not even answer to me"

The continuity between these rebrands is apparent in the Skype profile for Alien Spy, shown below in Figure 9.

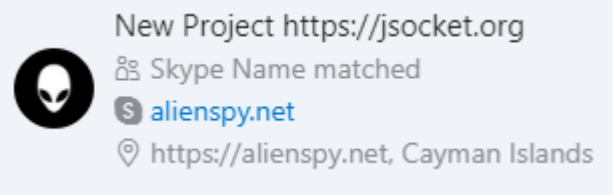

Figure 9. Alien Spy Skype profile

JSocket

The domain for this next rebrand, jsocket[.]org, was registered April 20, 2015 – 12 days after the Fidelis report. As of August 2019, it was still registered, although the domain hasn't resolved to an active website since early 2016.

Figure 10 shows some noticeable similarities between this site and its predecessor.

Figure 10. Comparison of alienspy[.]net and jsocket[.]org sites

In February 2016, unsubstantiated rumors that the Adwind author had been arrested circulated on forums.

On February 8, 2016, Kaspersky published a report on JSocket.

JBifrost

Our actor again responded quickly to the publication of the Kaspersky research on February 8, 2016. A new domain, jbifrost[.]com, was registered just two days later, on February 10, and jsocket[.]org, after replacing their website with a claim of spamming users being banned and legal issues, ceased to resolve after February 13, 2016.

Figure 11. JBifrost RAT logo

This incarnation of the site seemed to drop the loud public advertising in favor of a members-only private site with forums, sales, and chat.

The website was reported to have been suspended by the ISP in late-June 2016, and Fortinet published research into jBifrost on August 16, 2016.

Unknow(n) RAT

The actor appears to have taken a little longer in re-establishing his site after the jbifrost[.]com suspension. Unknowsoft[.]com was registered August 2, 2016, about a month after jbifrost[.]com was suspended during summer 2016. Again, this site supported a private members area rather than loud, public advertising.

Figure 12. Unknown RAT logo

The logo used for this rebrand, seen in Figure 12, is essentially unchanged from that of the previous jBifrost, shown in Figure 11, which wouldn't be expected had this business actually changed hands and truly rebranded.

The site was parked by the registrar August 4, 2017 and expired in December 2017. The registrar had previously suspended the site in late-September 2016, but the registration of Unknow(n) RAT's successor domain in December 2016 sets our milestone for the transition to the next rebranding.

jConnectPro

The last known possible website for the Adwind family, jconnectpro[.]info, was registered on December 10, 2016.

The site helpfully documented the connection and evolution of the malware family, shown in Figure 13.

"AlineSpy >> jSocket >> jBifrost >> UnknownSoftware >> jConnectPro"

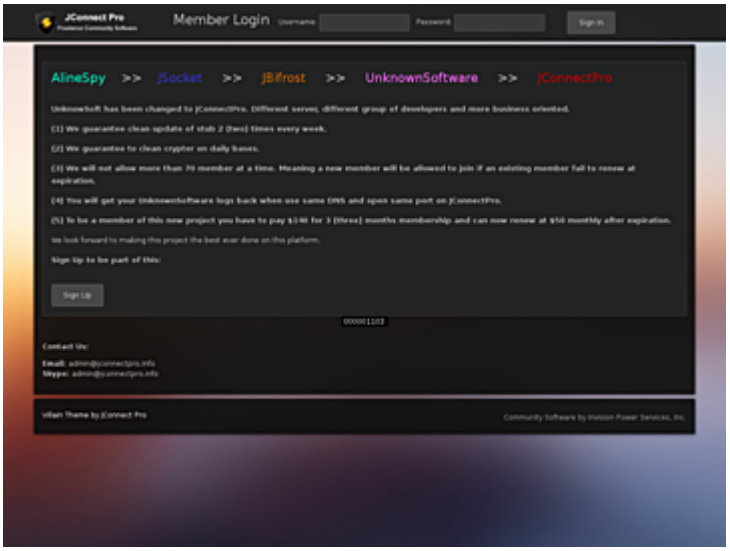

Figure 13. jconnectpro[.]info

The jConnect Pro site seen in Figure 13 bore an obvious similarity to the previous Unknown RAT site as shown in Figure 14. The site was suspended by the ISP in early April 2017.

It is possible that jconnectpro[.]info was NOT run by Adwind but rather was an imposter, selling a cracked version of Unknown RAT. Prior to ISP suspension, the Unknown RAT site unknowsoft[.]com posted an announcement that they were not taking any new customers, though the software would still operate, shown in Figure 14.

"Unkonown Software is currently unavailable

Not new users or renews in this moment. You can continue to use our software but you will not be allowed to login in our website.

Each membership of users will continue active until this expire.

Enjoy! And Good luck for ever.

Mastermind Team. We can just say good bay for ever.

We finished our work here since our software was selled to other team of developers. I don't know if they will continue or not. But we will try to update stub for currents users with active memberships."

A litany of complaints against purported fakes and scammers followed. Of special note:

"*http://jconnectpro[.]info – a FAKE"*

The timeline of RAT rebrand names at the site contains capitalizations in the names that differ from the original sites.

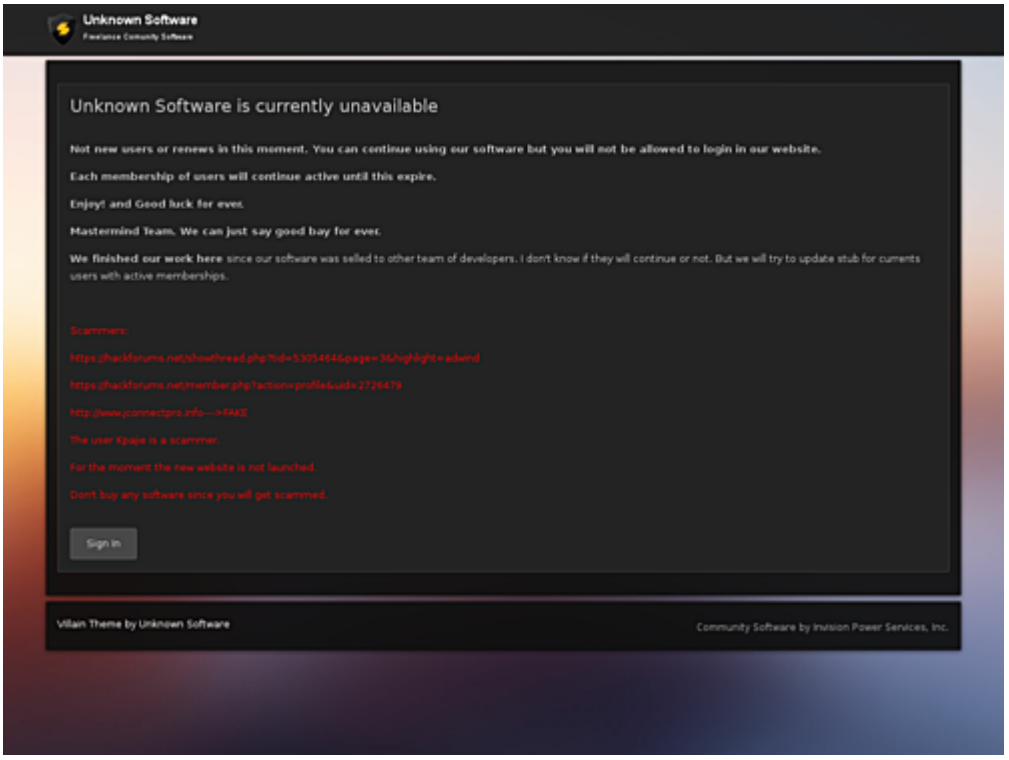

Figure 14. Unknown Software "unavailable"

A *Crypt*ic Puzzle

After unknownsoft[.]com and jconnectpro[.]info went down, Adwind's trail went cold. Although this time we were unable to find a newly rebranded iteration of Adwind's RAT, we did find a Java-RAT-specific crypting service.

Malware operators use a technique known as "crypting" to avoid signature-based antivirus detection. Crypting will modify malware binary files such that they have a new, unique hash value, without altering their functionality. Such files are often referred to as "fully undetectable" (FUD).

There are comparatively few Java-specific commodity RATs, and this crypting service seemed to adopt UnknownRAT's name in its branding – UnknownCrypter (unknowncrypter[.]co) (Figure 15).

Figure 15. UnknownCrypter

Initial investigation uncovered some Spanish-language artifacts associated with UnknownCrypter. We wondered if Adwind might be leveraging his Java coding expertise and operating this system himself as a second revenue stream alongside his RAT.

However, our research determined that this was simply a rebranding of the "FUDCrypter" service, operated by a Nigerian individual, not Adwind.

In our SilverTerrier research of Nigerian cybercrime, we note an increase in the popularity of commodity RATs among that community. Indeed, our research into leaked customer lists of commodity malware has shown that the vast majority of the customers are Nigerian. We also observed a burgeoning Nigerian ecosystem around the various aspects of cybercrime, and so a Nigerian-based crypting service should not come as a surprise.

Further confirming our conclusion that this is not operated by Adwind, the same actor recently launched his own JavaScript-based RAT called "WSH RAT" with a very different codebase – a competitor to Adwind rather than a new iteration of Adwind's RAT.

Cracked

Although Adwind apparently no longer sells his RAT on the web or on forums, the question remains: what of all the ongoing Adwind-family telemetry do we continue to observe?

Cracked copies of Adwind-family malware have been in circulation for several years, through to cracked versions of Unknown RAT as seen in Figure 16.

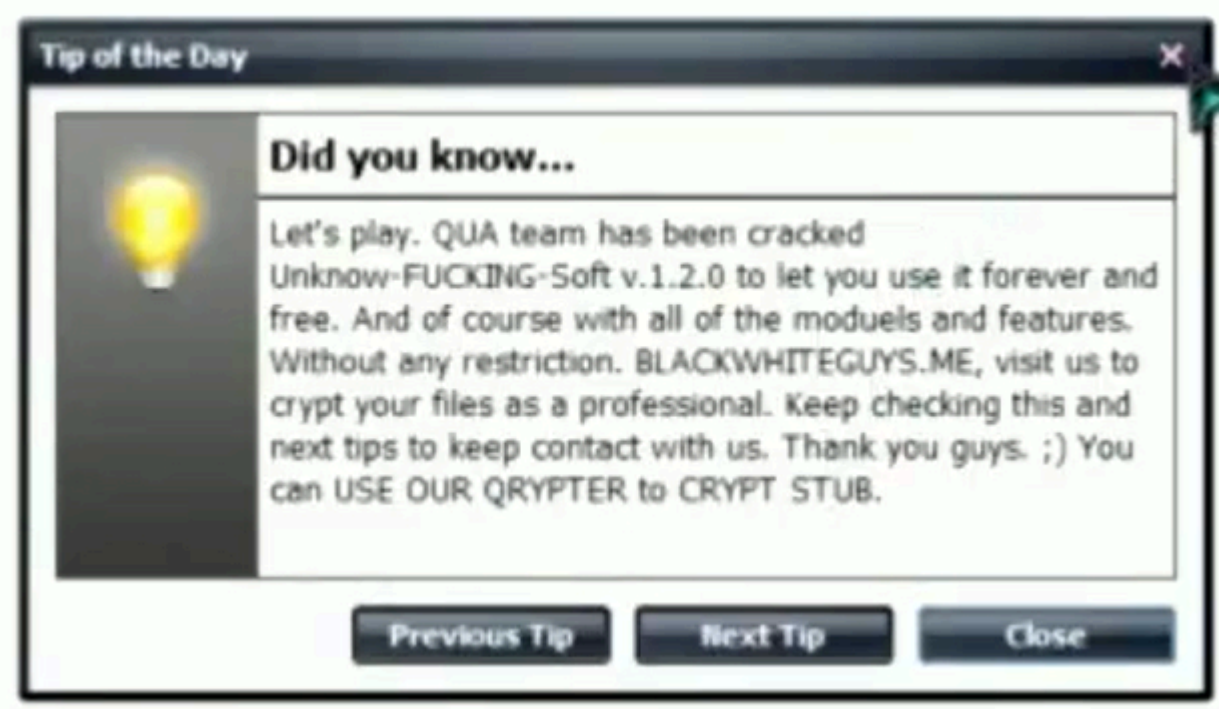

Figure 16. Cracked Unknown RAT

We first observed Adwind-family samples add a registry entry for the BullGuard binary "LittleHook.exe" into their anti-antimalware routine on December 5, 2016. This corresponds closely with the ostensible rebranding to jConnectPro, with that domain being registered only five days later.

Although we noted earlier that jconnectpro[.]info may potentially not actually belong to Adwind, we are able to use this marker to differentiate between "legitimate" and cracked Adwind samples. All known cracked versions of Unknown RAT predate the above-observed branding and domain change.

Since December 2016, we have collected 14,000 "legitimate" samples, observed in over 600,000 attacks against Palo Alto Networks customers. Cracked versions of earlier Adwind family RATs seem to be twice as common. During the same period, we found almost 30,000 Adwind samples that did *not* contain that marker, observed in over 1.3 million attacks against Palo Alto Networks customers.

Gone Dark?

As we noted earlier, the jConnectPro website was suspended in early April 2017. Unknownsoft[.]com had an "unavailable" statement at the site, ISP suspensions from 2016, and was finally parked mid-2017. Unlike previous rebranding, there was no handoff to a new brand as we had observed earlier, via website, Skype, forum, or reports of emails to customers. There was no "new Adwind" advertising on forums. This begged the question: Has Adwind finally closed up shop? Is the ongoing Adwind telemetry simply observing cracked versions and legacy legitimate samples continuing to be deployed?

We found that Adwind samples first started setting the registry key "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ProcessHacker.exe\debugger , Value:svchost.exe , Type:1" in samples starting June 5, 2017. This was two months after the jConnectPro website was suspended, and Unknown

Software was “unavailable” and the site suspended – the first proof of ongoing development of the RAT subsequent to having gone dark.

We noted some other small changes in file writes in samples around this date, but we have not been able to identify any other new functionality in samples observed since June 2017. Samples with these markers continue to be observed in the active attacks through September 2019.

A Tale Is Woven

Our analysis of Adwind’s infrastructure throughout the different brands of his RAT found uncommonly good operational security (OpSec) on his part. WHOIS records were fake and/or anonymized. Domain registrars and hosting services were distinctly changed with every rebrand. Infrastructure was not reused. No careless connections to other activity that might hint at Adwind’s identity were found.

Having analyzed thousands of actors and their infrastructure, such consistently good OpSec is a rarity. Adwind attempted not only to hide his identity but, fearing discovery and in order to distance himself from issues with bad reputation, also attempted to suggest a change of ownership.

In his attempt to misdirect identification and pretend to have on-sold his business, Adwind inadvertently left a pattern in his OpSec. The very consistency of his OpSec itself is an indicator of it remaining under his control during its entire history.

Despite the renaming, the RAT itself really didn’t change significantly over its lifetime. Some new functionality was added, but improvements were essentially iterative. No significant changes were noted, as might be expected with a new owner/coder, and Java commodity RATs remain comparatively rare.

Care was always taken to ensure a continuity between brands for his customers; the new brand was noted in forums on the old website, in his Skype profiles (Figure 9), and in emails to existing customers – more care than might be expected if it was on-sold to a third party.

Domain moves were always seamless, and rebrands were, on several occasions, clearly triggered by the publishing of research (Figure 17). Even after the claimed “sale,” UnReCom still had predominant Mexico hosts in screenshots (Figure 6).

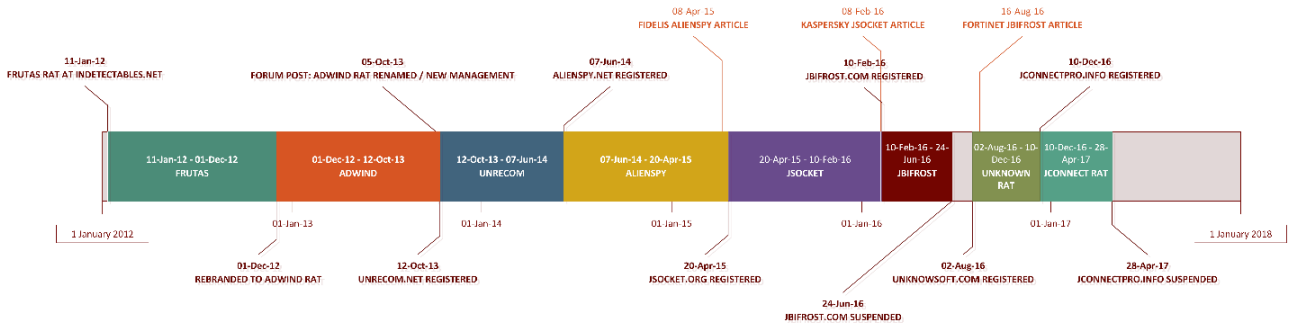

Figure 17. Timeline of the Adwind RAT family

Stylistic similarities bridged the different RAT brands – logos (Figures 11 and 12), site content (Figures 13 and 14) and also as seen above in the jSocket section. In fact, the only "rebrand" that carries doubt that it actually belonged to Adwind was jconnectpro[.]info – the timeline has the "unavailable" unknownsoft[.]com overlapping the same timeframe and calls jconnectpro[.]info "*a FAKE*".

Who Is 'Adwind'?

As we noted earlier, Adwind has uncommonly good OpSec, and initially, conclusively identifying him through his infrastructure wasn't possible.

Spanish-language artifacts were obvious early on. The original website selling Adwind was adwind[.]com[.]mx, and several YouTube videos and screenshots showed a predominance of Mexican host computers (Figure 18).

Figure 18. Mexican host computers in YouTube advertising

The email address adwind[at]live.com is found in the strings of Frutas samples (Figure 19) and was referenced at a YouTube video promoting Adwind 1.0.

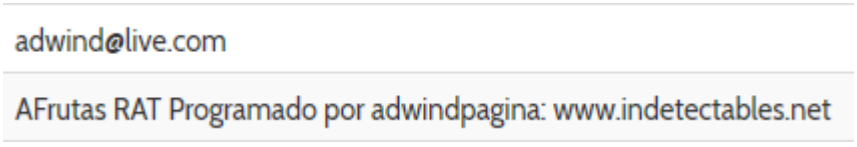

Figure 19. Frutas strings

This email address is associated with a Skype profile "adwindandres" (Figure 20), which includes the Adwind logo.

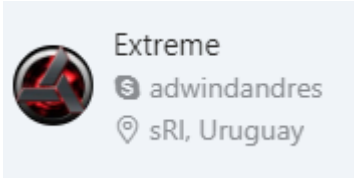

Figure 20. Skype profile

That Skype profile was also used at hackforums[.]net to sell early versions of Adwind RAT. It was also the Skype listed at the original Adwind website (Figures 3 and 21).

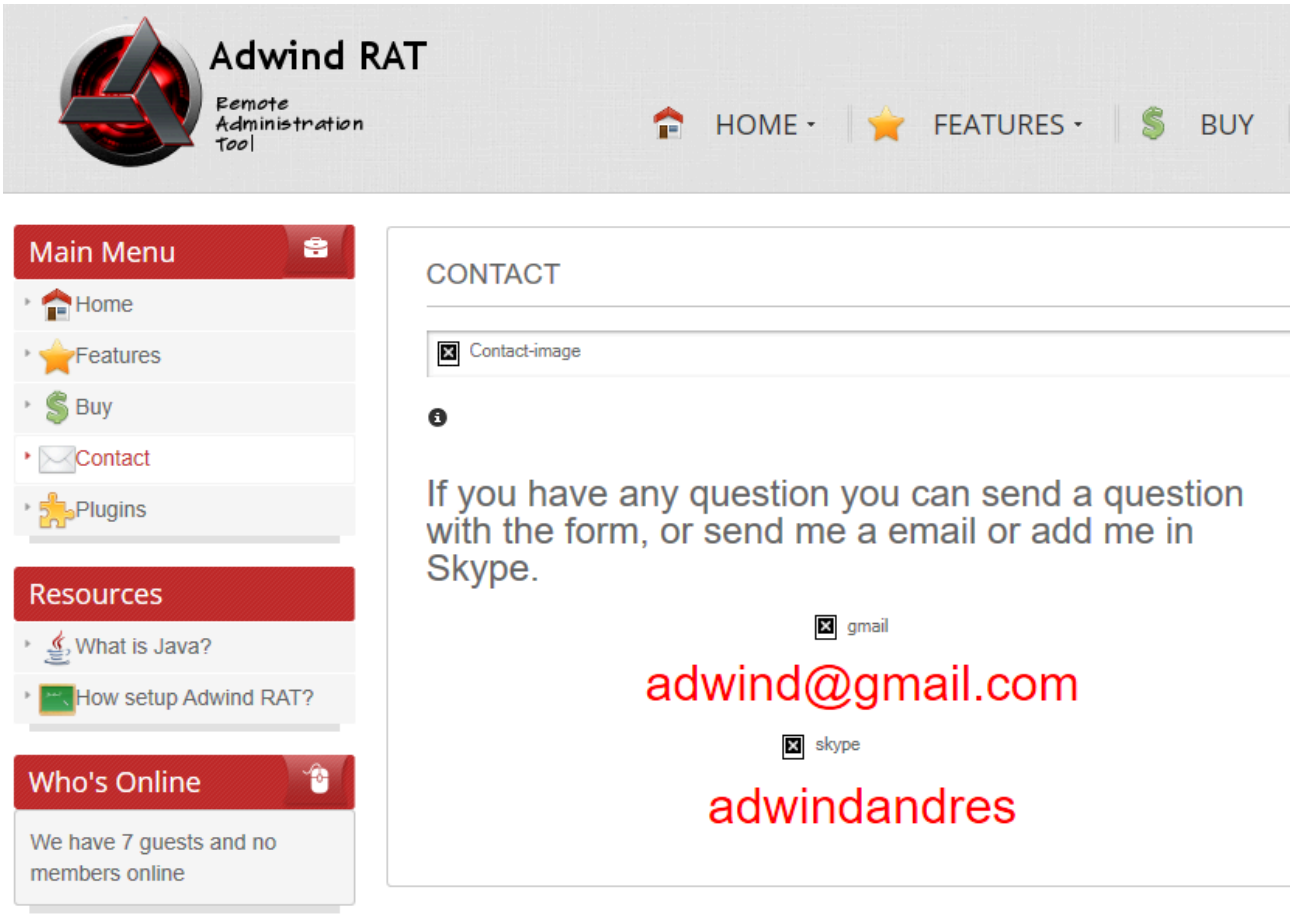

Figure 21. Original Adwind site Skype

The same email address is also found in an academic paper, with the same name “Andres” as noted in the Skype:

“C. M. Andrés is a student from J[redacted] Autonomous University of T[redacted] in Mexico in the last semester of the degree in computer systems; (email: adwind [at]live.com).”

Elsewhere the paper mentions his full name.

The very first historical WHOIS entry for adwind[.]com[.]mx contained a full name and location, which matches the name and location in the academic paper. The WHOIS record was changed to fake information shortly thereafter.

Name: Andres A[redacted] C[redacted] M[redacted]

City: C[redacted]

State: T[redacted]

Country: Mexico

The full name of Adwind Andrés appears to be unique. Research uncovered other references to him studying information systems at that university.

It also led to his Google Maps reviewer profile (Figure 22). The 4,000+ reviews in that profile, including up until a few weeks prior to publication of this blog post, suggest that Adwind Andrés now resides in C[redacted], Mexico – a few hours drive from his university.

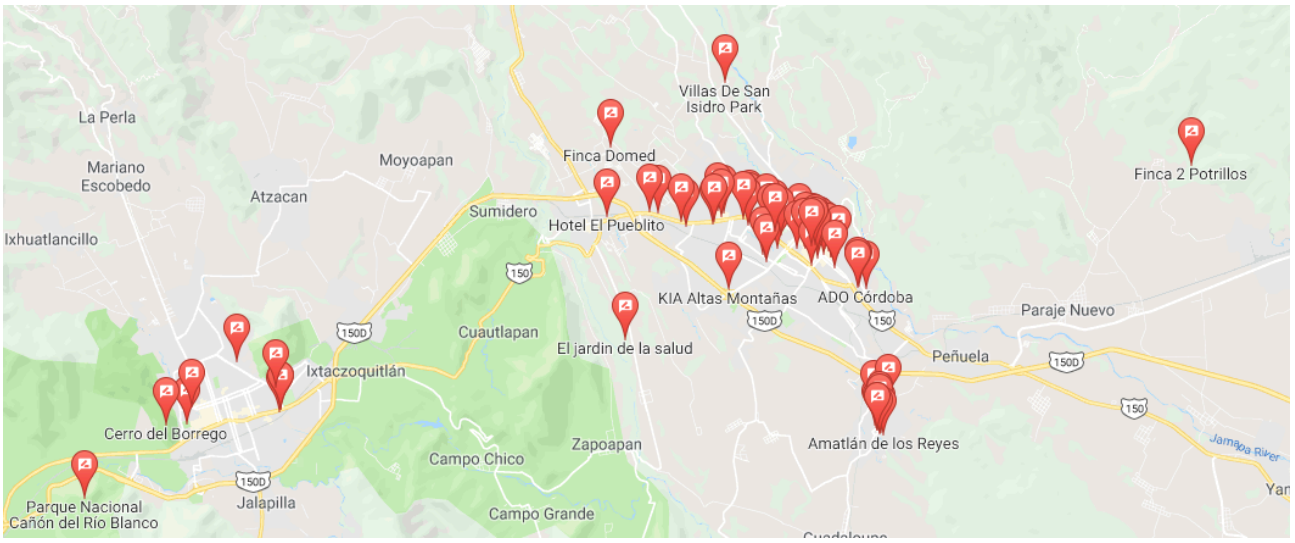

Figure 22. Google Maps reviews

A Never-Ending Story?

The ready availability of commodity malware empowers a huge population of unsophisticated threat actors, who would otherwise lack the technical ability to code their own malware. Although the author might not financially benefit from the spread of cracked versions of the malware, the author is, after all, responsible for its original existence.

Distributed since 2012, sale of the Adwind RAT family has resulted in tens of thousands of malware samples in the wild and millions of malware attacks.

Over the last eight years, Adwind Andrés has unsuccessfully attempted to hide his identity as the author of this malware and distance himself using successive rebrands.

As he has iteratively continued to improve upon his software, it would seem that he has been driven into a private-customer model. However, to this day, he continues to develop this software, and profit from its sale to malware actors.

Organizations with good 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 the Adwind RAT family malware with WildFire and Traps. AutoFocus users can track this activity using the Adwind tag.

Palo Alto Networks has shared our findings, including file samples and indicators of compromise, in this report with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit www.cyberthreatalliance.org.
