Recorded Future

CYBER THREAT ANALYSIS

Bestsellers in the Underground Economy:

Measuring Malware Popularity by Forum

By Insikt Group®

Recorded Future's Insikt Group® analyzed advertisements and comments within underground forums to determine popular malware and malware categories within underground forums. Sources include the Recorded Future® Platform, as well as open web, dark web, and underground forum research.

This report will be of greatest interest to organizations seeking to better understand malware dissemination within the criminal underground, as well as those who wish to monitor developing malware-related criminal threats.

Executive Summary

By analyzing over 3.9 million posts from May 2018 to May 2019 across all underground forums indexed by the Recorded Future platform, Insikt Group identified the top malware variants being referenced on underground forums. Insikt Group also attempted to find real-world events that correlated with a higher number of malware references on these forums, as well as differences in tools advertised in forums of different languages, to see if any differences existed.

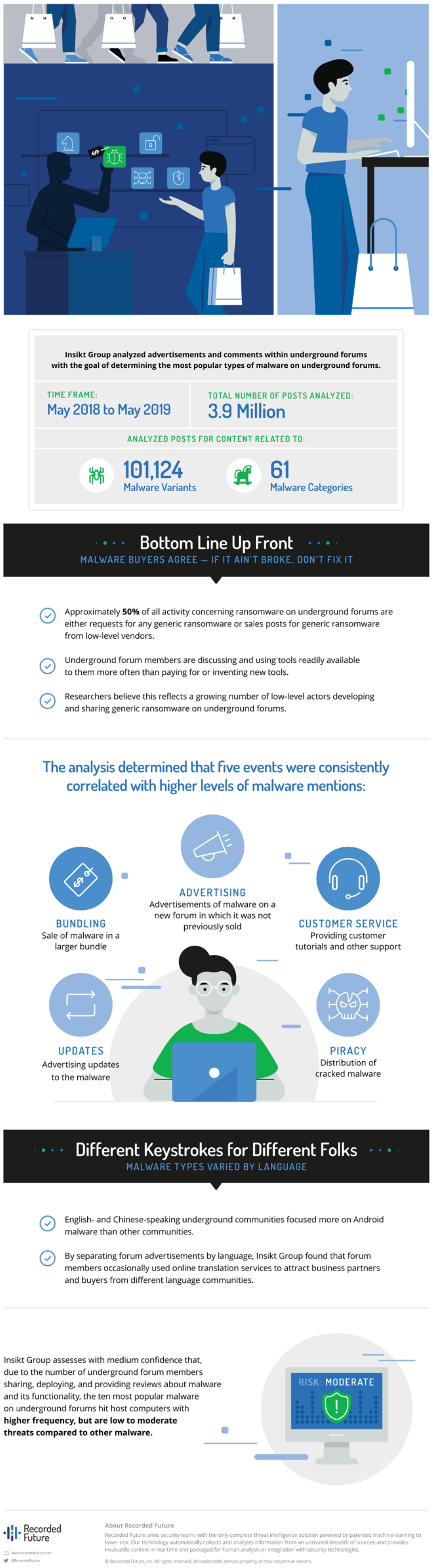
Insikt Group discovered that a majority of the top 10 mentions of malware in multiple languages included openly available dual-use tools, open-source malware, or cracked malware. Some of these malware families were also over three years old or could be mitigated with basic security precautions. Activity in underground forums that correlated to growth in malware references included: sale of malware in a larger bundle, advertising updates to the malware, advertisements of the malware on a new forum in which the malware was not previously sold, news articles related to malware shared on forums, and community engagement.

Insikt Group also discovered that underground communities in different languages did indeed focus on different malware, malware categories, and attack vectors. English- and Chinese-speaking underground communities, for example, focused more on Android malware than other communities. By separating forum advertisements by language, Insikt Group found that forum members occasionally used online translation services to attract business partners and buyers from different language communities.

Key Judgments

- The top 10 mentions[1] of malware across Recorded Future underground forum collections suggest that underground forum members are discussing and using tools readily available to them more often than paying for or inventing new tools.
- Based on the prevalence and longevity of the malware, Insikt Group assesses with medium confidence that there likely exist enough victims who do not comply with basic security precautions for forum members to successfully infect.
- Approximately 50% of all activity concerning ransomware on underground forums are either requests for any generic ransomware or sales posts for generic ransomware from lower-level vendors. We believe this reflects a growing number of low-level actors developing and sharing generic ransomware on underground forums.
- Insikt Group assesses with medium confidence that, due to the number of underground forum members sharing, deploying, and providing reviews about malware and its functionality, the 10 most popular malware on underground forums hit host computers with higher frequency, but are low to moderate threats compared to other malware due to their age, ineffectiveness without a delivery vehicle or crypter, and existing antivirus detections.

[1] Insikt Group defines "mentions" as a Recorded Future "reference." This is either a post that contains an exact text match of an entity (in any language that Recorded Future analyzes), or a text match of a synonym, nickname, or abbreviation of that entity.



Insikt Group analyzed advertisements and comments within underground forums with the goal of determining the most popular types of malware on underground forums.

TIME FRAME: May 2018 to May 2019	TOTAL NUMBER OF POSTS ANALYZED: 3.9 Million

ANALYZED POSTS FOR CONTENT RELATED TO:

101,124 Malware Variants	61 Malware Categories

Bottom Line Up Front

MALWARE BUYERS AGREE — IF IT AIN'T BROKE, DON'T FIX IT

- ✓ Approximately **50%** of all activity concerning ransomware on underground forums are either requests for any generic ransomware or sales posts for generic ransomware from low-level vendors.
- ✓ Underground forum members are discussing and using tools readily available to them more often than paying for or inventing new tools.
- ✓ Researchers believe this reflects a growing number of low-level actors developing and sharing generic ransomware on underground forums.

The analysis determined that five events were consistently correlated with higher levels of malware mentions:

BUNDLING
Sale of malware in a larger bundle

ADVERTISING
Advertisements of malware on a new forum in which it was not previously sold

CUSTOMER SERVICE
Providing customer tutorials and other support

UPDATES
Advertising updates to the malware

PIRACY
Distribution of cracked malware

Different Keystrokes for Different Folks

MALWARE TYPES VARIED BY LANGUAGE

- ✓ English- and Chinese-speaking underground communities focused more on Android malware than other communities.
- ✓ By separating forum advertisements by language, Insikt Group found that forum members occasionally used online translation services to attract business partners and buyers from different language communities.

Insikt Group assesses with medium confidence that, due to the number of underground forum members sharing, deploying, and providing reviews about malware and its functionality, the ten most popular malware on underground forums hit host computers with **higher frequency, but are low to moderate threats compared to other malware.**

Recorded Future
www.recordedfuture.com
@RecordedFuture

About Recorded Future
Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.

Background

In the last year, Recorded Future has reported on the hacking communities within Russia, China, Iran, and Brazil. This research draws special attention to what malware is popular within those communities. In order to better understand commodity malware that may be targeting client environments, we used a data-driven approach to answer the following questions:

- What are the top 10 malware variants being discussed on underground forums?
- Do underground forums in different languages advertise different tools? What kinds of differences or similarities can we see?
- What events occur in either real life or underground forums that result in higher malware references? Effectively, what makes certain malware variants grow in popularity?

Methodology, Definitions, and Limitations

From May 1, 2018, to May 1, 2019, Insikt Group researchers pulled all mentions of any malware family or category by month from underground forums spanning the dark web, the open web, and related sources. Insikt Group gathered over 3.9 million posts and checked the posts for mentions of 61 malware categories and 101,124 malware names.

The definition of malware used in this report is "operational pieces of code used to conduct illegal activity." This expanded the scope of the data set to include vague categories (e.g., botnet, crypter, or webshell), red-teaming tools, or even certain exploits, such as ETERNALBLUE. While these entities are not usually classified as malware, individuals in both underground markets and forums talk about these entities similarly enough to malware to be notable, as shown by the data in the "Threat Analysis" section below.

There were four limitations inherent within the data set:

1. As Recorded Future continues to expand its analysis to include new sources every month, and as forums change domains (either due to takedowns or as they add additional redundancies), it is likely that we have missed small amounts of data.
2. A portion of the mentions in the data set were reposts of news articles and security research. However, we believe that those posts are still valuable, as hackers can occasionally get inspiration from other families of malware to create variants or exploit newer attack vectors. Therefore, we left them in the data set.
3. Individuals posting on forums would post in their non-native language if the forum operated primarily in a certain language, or if the individual wanted to attract buyers from a specific country. Therefore, certain language-based data was inherently skewed.
4. Certain posts mentioning malware were spam posts that mentioned the names of many different families of malware or tools. This was a tactic used by forum members advertising new marketplaces in order to show up in more search results. When a majority of malware mentions over the year could be attributed to this phenomenon, the entity was struck from the data set.

Threat Analysis

Malware Mentions by Language

After gathering the data, we separated the number of mentions over the 13 months by eight languages, and turned the top 10 mentions of malware by language into bar graphs (for the full set of graphs, see Appendix B).

Overall, we observed that a majority of the top 10 graphs included openly available dual-use tools, such as MinerGate and Imminent Monitor (a cryptominer and a remote-access tool, respectively, created initially for legitimate uses), and open-source malware, such as njRat, AhMyth, and Mirai. This likely demonstrates that underground forum members are eager to discuss and use tools readily available to them rather than pay for or invent new tools. Many of the non open-sourced entities mentioned, like SpyNote, Trillium, NLBrute, and RDPBrute, had been previously cracked, meaning that multiple forum members now distribute unauthorized copies of the malware, usually at cheaper prices than the original seller.

The top 10 graphs also included malware that had been around for over three years, like Gh0st RAT, in addition to malware that is usually detectable with antivirus software or thwarted with good password hygiene. For example, RDPBrute (and its variants) will brute-force usernames and passwords on IPs with open RDP ports to gain initial access on a machine. This tool could be easily thwarted with difficult passwords, or by turning off RDP entirely. However, forum members continue to use this tool (and others) regardless, suggesting that they have been able to successfully infect victim hosts with the above malware.

Additionally, the graphs included tools designed to conduct other illegal activity, such as account stuffing, spamming, or carding. For example, Xrumer is software that allows criminals to spam multiple forums and forum comments with similar posts in an attempt to improve their results on forum search engines, or even regular search engines on the open web.

We discovered several pieces of malware that were discussed broadly within multiple language groups, including:

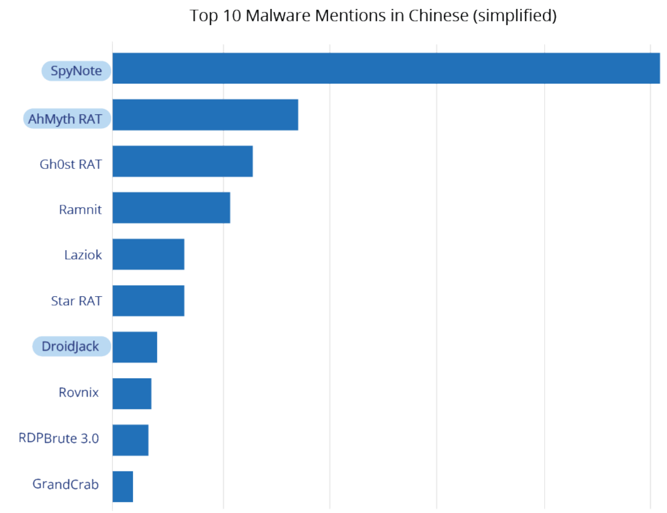
1. njRat, a windows RAT created in late 2012, the source code of which is available online on certain forums. This RAT is popular in English, Arabic, Spanish, Russian, Chinese (traditional), and Farsi posts.

2. SpyNote, an openly available Android-based RAT containing keylogging and GPS functionality. This application was found on malware forums starting in 2016. This RAT is popular in English, Chinese (simplified), Chinese (traditional), Spanish, Japanese, and Arabic posts.
3. GandCrab, a ransomware made famous by its namesake author, discovered in early January 2018. GandCrab's primary vendors retired in June 2019, and the FBI released the master decryption keys for versions 4, 5, 5.04, 5.1 and 5.2 in July 2019. This ransomware is popular in Russian, Chinese (simplified), Spanish, Farsi, and Arabic posts.
4. DroidJack, an Android RAT created in 2014 with an official website that sells lifetime licenses for $210, but with cracked versions for far cheaper on underground forums. This RAT is popular in Chinese (simplified), Chinese (traditional), English, and Arabic posts.

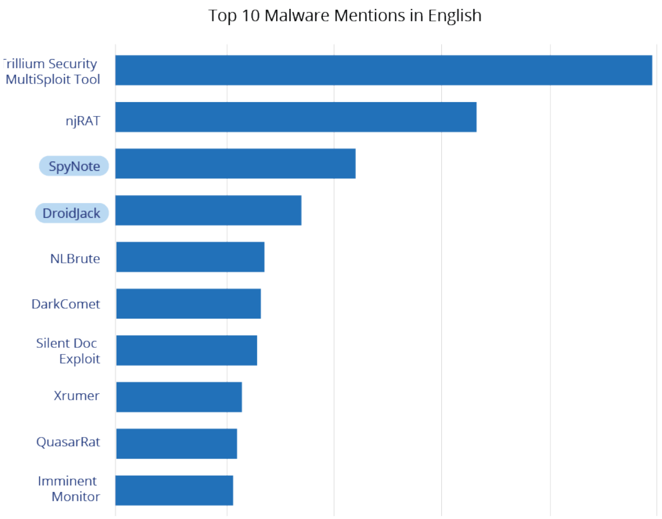
Analysis of Malware Popularity by Language

While many of the malware presented in our analysis had similar characteristics, each bar graph contained remarkably different content, showing that underground forums of different languages focus on different families of malware. Mentions of Nanocore, a cheap and easy-to-use remote-access trojan, were discussed more frequently on Farsi and Japanese forums. Xrumer had a high number of references on Russian forums and far fewer references on English forums, but was found in no other languages. The top malware entity mentioned in English-speaking forums was Trillium Security Multisploit Tool, which has only shown up a handful of times in forums containing other languages.

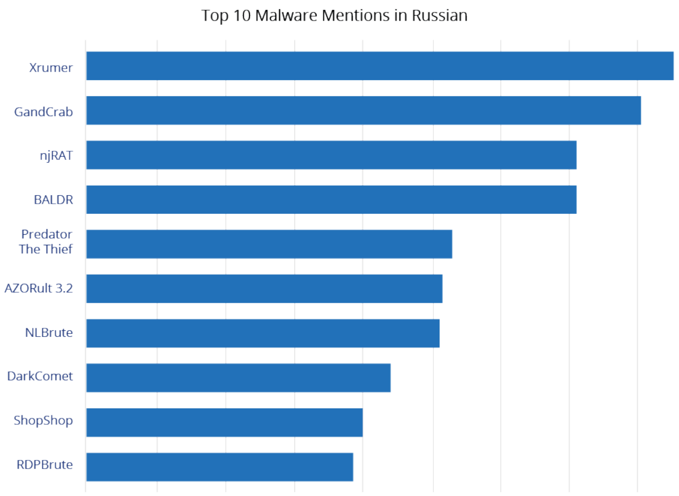
Additionally, the data shows that underground forums of different languages focus on different targets and attack vectors. For example, Chinese- and English-speaking underground forums focus more on targeting Android devices than their Russian counterparts. The top 10 malware within the Chinese-speaking underground included three Android trojans: SpyNote, AhMyth, and DroidJack. The English-speaking underground included two of those three: SpyNote and DroidJack. This is in stark contrast to the Russian-language group, whose top 10 contains no mobile malware whatsoever.



Top 10 malware mentions in Chinese (simplified).

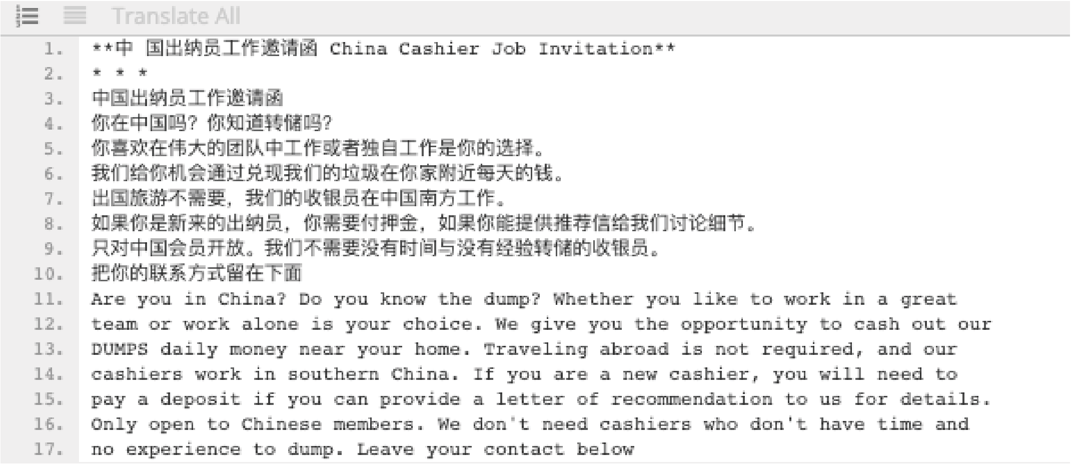


Top 10 malware mentions in English.



Top 10 malware mentions in Russian.

As mentioned in the research limitations outlined above, certain language-based data was inherently skewed, as individuals posting on forums would post in their non-native language if the forum operated primarily in a certain language (for example, a Russian forum member posting in English on an English-language forum), or if the individual wanted to attract buyers from a specific country. The latter discovery adds an additional layer to our previous research comparing Chinese and Russian underground forums, in which Recorded Future found that Russian- and English-language forums also contained Chinese-language posts, and assessed that Chinese forum members were likely advertising services to other Chinese individuals on non-Chinese forums. While certain posts on non-Chinese forums were written in native Chinese, other forum posts were likely non-Chinese individuals using Google Translate to attract Chinese- or English-speaking business partners and buyers.



```
**中 国出纳员工作邀请函 China Cashier Job Invitation**
* * *
中国出纳员工作邀请函
你在中国吗？ 你知道转储吗？
你喜欢在伟大的团队中工作或者独自工作是你的选择。
我们给你机会通过兑现我们的垃圾在你家附近每天的钱。
出国旅游不需要，我们的收银员在中国南方工作。
如果你是新来的出纳员，你需要付押金，如果你能提供推荐信给我们讨论细节。
只对中国会员开放。我们不需要没有时间与没有经验转储的收银员。
把你的联系方式留在下面
Are you in China? Do you know the dump? Whether you like to work in a great
team or work alone is your choice. We give you the opportunity to cash out our
DUMPS daily money near your home. Traveling abroad is not required, and our
cashiers work in southern China. If you are a new cashier, you will need to
pay a deposit if you can provide a letter of recommendation to us for details.
Only open to Chinese members. We don't need cashiers who don't have time and
no experience to dump. Leave your contact below
```

Post on an underground forum in poorly-translated Chinese and English. (Source: Recorded Future)

Measuring Malware Popularity

While mentions of malware is useful data to analyze in some regard, raw mentions do not count comments on a forum post about the family of malware, which usually represent other individuals that are interested in buying or discussing the malware.

To address this issue, Insikt Group measured malware popularity using the following metrics:

1. **Total Number of Raw Mentions** *(R)*: Any time a family of malware was mentioned on a forum, regardless of whether the mention was part of a new post or a reply on a forum thread.
2. **Total Number of Replies on a Thread** *(T)*: Any reply to an initial post mentioning a family of malware would be counted toward said malware, as the act of replying to a post related to a malware family is usually user engagement on that malware family, regardless of whether the comment mentions the malware.

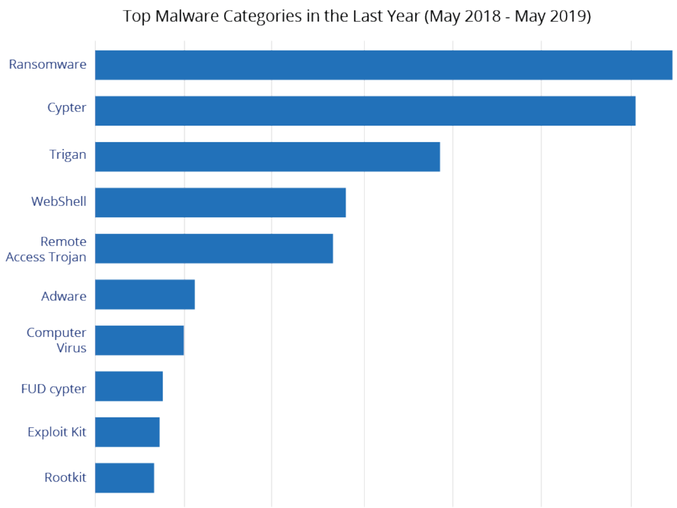
The complete equation for the popularity of a single family of malware across X number of underground forums is as follows:

$$\sum_{a=1}^{X} \left(T_a + R_a\right)$$

Effectively, for every forum, the sum of every mention and thread reply related to the malware in a single forum would be calculated. The sums for each forum would then be added together to get the total popularity.

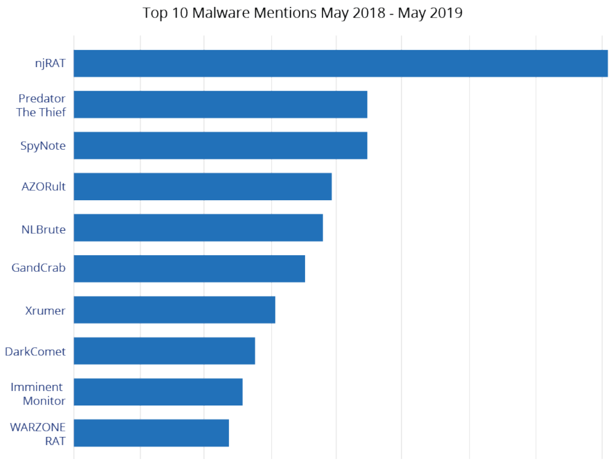
Popularity Analysis Results

By calculating metrics using the equation with the data previously gathered, Insikt Group was able to obtain the results shown below.



Top 10 malware category mentions overall.

From May 2018 to May 2019, the top malware category mentioned in underground forums was ransomware, followed by crypter, and finally, trojan (with approximately two-thirds as many mentions). While "botnet" is not a malware category in a technical sense, botnets had more than twice as many mentions as ransomware. Based on the data, Insikt Group assesses that a large portion of individuals on underground forums likely still collect and use botnets for a variety of illicit activity, including DDoS attacks, cryptomining, fraud, and sending spam.



Top 10 malware strain mentions overall.

Of the top 10 malware mentions over all indexed forums, five (njRAT, SpyNote, DarkComet, Imminent Monitor, and WARZONE RAT) are remote-access trojans, two (Predator the Thief and AZORult) are information stealers, one is a tool used for initial access to a victim (NLBrute), and one (Xrumer) is a forum-specific tool.

Additionally, while "ransomware" was the top malware category mentioned on underground forums in the last year, it is worth noting that only one of the top 10 specific malware strains mentioned, GandCrab, is a ransomware strain. Out of the top 150 strains of malware collected, only 11 were ransomware, as shown in the table below. Approximately 50% of the mentions on underground forums in the past year were discussions and sales posts on generic, lower-level ransomware that do not have names or branding. This supports a previous analysis that Recorded Future published on this topic, looking toward 2019 ransomware trends.

6: GandCrab	30: WannaCry	51: Cryptolocker	73: Princess Locker
84: Petya	88: NotPetya	110: Relock	124: Saturn Ransomware
125: Samsam	133: Ryuk Ransomware	144: Rapid Ransomware	

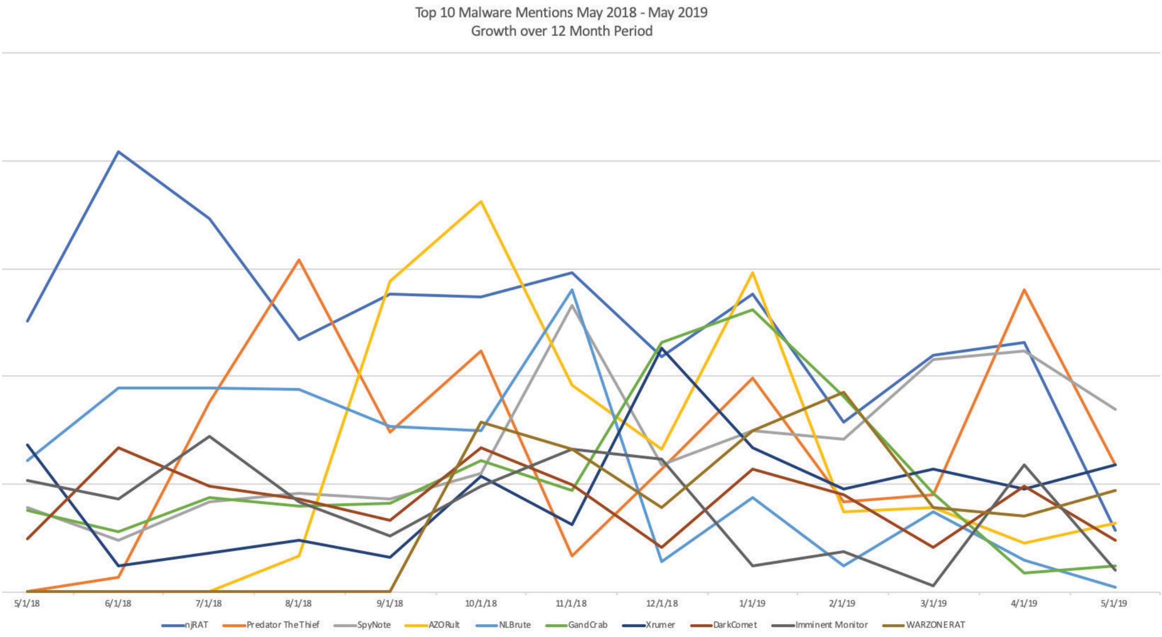
Named ransomware within the data set of the top 150 malware strains collected.

Technical Analysis

Correlations Between Real-World Events and Popularity Growth

The graph below illustrates the same top 10 strains of malware on underground forums, but separates the number of posts by month. As shown in the graph, our analysis indicates that the families of malware that were discussed most frequently over the course of the year had different levels of engagement over the 13-month period. After taking a deeper dive into the content of the forum threads during the spikes in activity, we determined that five events were consistently correlated with higher levels of malware mentions:

1. The sale of malware in a larger collection or set
2. Advertising updates to the family of malware
3. Distribution of cracked malware versions
4. Real-world news articles
5. Community engagement with the malware

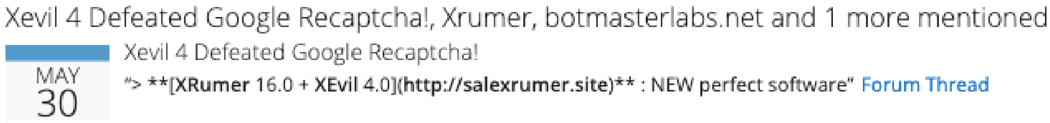


Most popular malware. (May 2018 to May 2019)

Malware Collection

Malware collections are multiple samples of different malware sold as a set, usually advertised as a collection of hacking tools that potential buyers can play around with to test which ones they like best. Of the references to malware collections found within the Recorded Future platform, the malware sold together were usually old or open-sourced malware already available on multiple forums. Because multiple malware variants were named in a collection's sales post, the post showed up in multiple different forum search queries, and individuals searching for disparate families of malware converged on that post.

For example, njRAT's greater number of references in June 2018 was correlated with a sales post for a "50 RAT Bundle" on now-defunct Dream Market, which contained builders for both families of malware. DarkComet and njRAT were both featured in a "561 RATs Collection" on a different forum in that same month. In addition, bundling tools that worked together also resulted in a spike in references. A post made on May 22, 2018 claimed that by using Xrumer (the forum spammer) alongside XEvil (a captcha checker), the actor was able to bypass over 8,400 captchas on forums, and most posts referencing Xrumer that were collected by Recorded Future in that month also referenced XEvil.



Xevil 4 Defeated Google Recaptcha!, Xrumer, botmasterlabs.net and 1 more mentioned

MAY
30

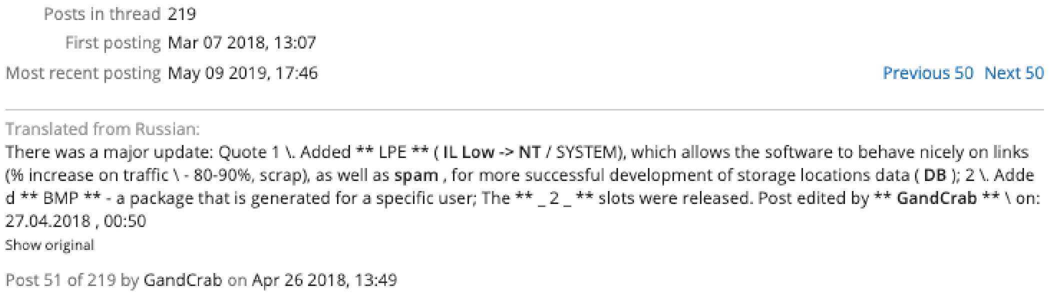
Xevil 4 Defeated Google Recaptcha!

"> **[XRumer 16.0 + XEvil 4.0](http://salexrumer.site)** : NEW perfect software" Forum Thread

Reference to XRumer and XEvil being sold as a package. (Source: Recorded Future)

Updates to Original Malware

Malware vendors on Russian- and English-language sites tended to either post comments on the original sales thread or create new sales threads containing updates to the original malware variant. By updating the malware, vendors could update their sales posts and create higher post exposure within the forum to attract additional buyers. This sales post update would, on many occasions, cause the sales thread to get bumped to the forum's front page. This is because many underground forums either sort forum threads by most recently active, or have a section advertising recently active comments or threads. GandCrab regularly announced updates to their namesake malware in this format.



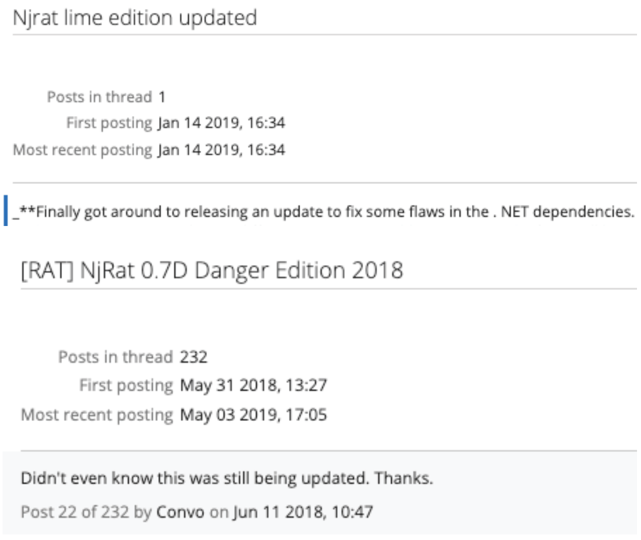
Posts in thread 219
First posting Mar 07 2018, 13:07
Most recent posting May 09 2019, 17:46

Translated from Russian:
There was a major update: Quote 1 \. Added ** LPE ** (**IL Low** -> **NT** / SYSTEM), which allows the software to behave nicely on links (% increase on traffic \ - 80-90%, scrap), as well as **spam** , for more successful development of storage locations data (**DB**); 2 \. Adde d ** BMP ** - a package that is generated for a specific user; The ** _ 2 _ ** slots were released. Post edited by ** **GandCrab** ** \ on: 27.04.2018 , 00:50

Post 51 of 219 by GandCrab on Apr 26 2018, 13:49

Comment on a forum thread made by GandCrab, announcing the GandCrab version 5 update. (Source: Recorded Future)

In addition, the spike in activity correlated with updating malware not only applied to proprietary malware vendors, but also to open source developers and vendors of cracked goods. For vendors of cracked goods, having a newer version of their product differentiated them from other vendors selling the same good. For open source developers, fixing issues and adding new features to an open source tool that they could then share on malware forums allowed them to sell their version of the tool or develop their reputation on a certain forum. For example, while njRAT is openly available on GitHub, multiple forums contained posts of different "njRAT editions" either being sold or given away for free.



Njrat lime edition updated

Posts in thread 1
First posting Jan 14 2019, 16:34
Most recent posting Jan 14 2019, 16:34

_**Finally got around to releasing an update to fix some flaws in the . NET dependencies.

[RAT] NjRat 0.7D Danger Edition 2018

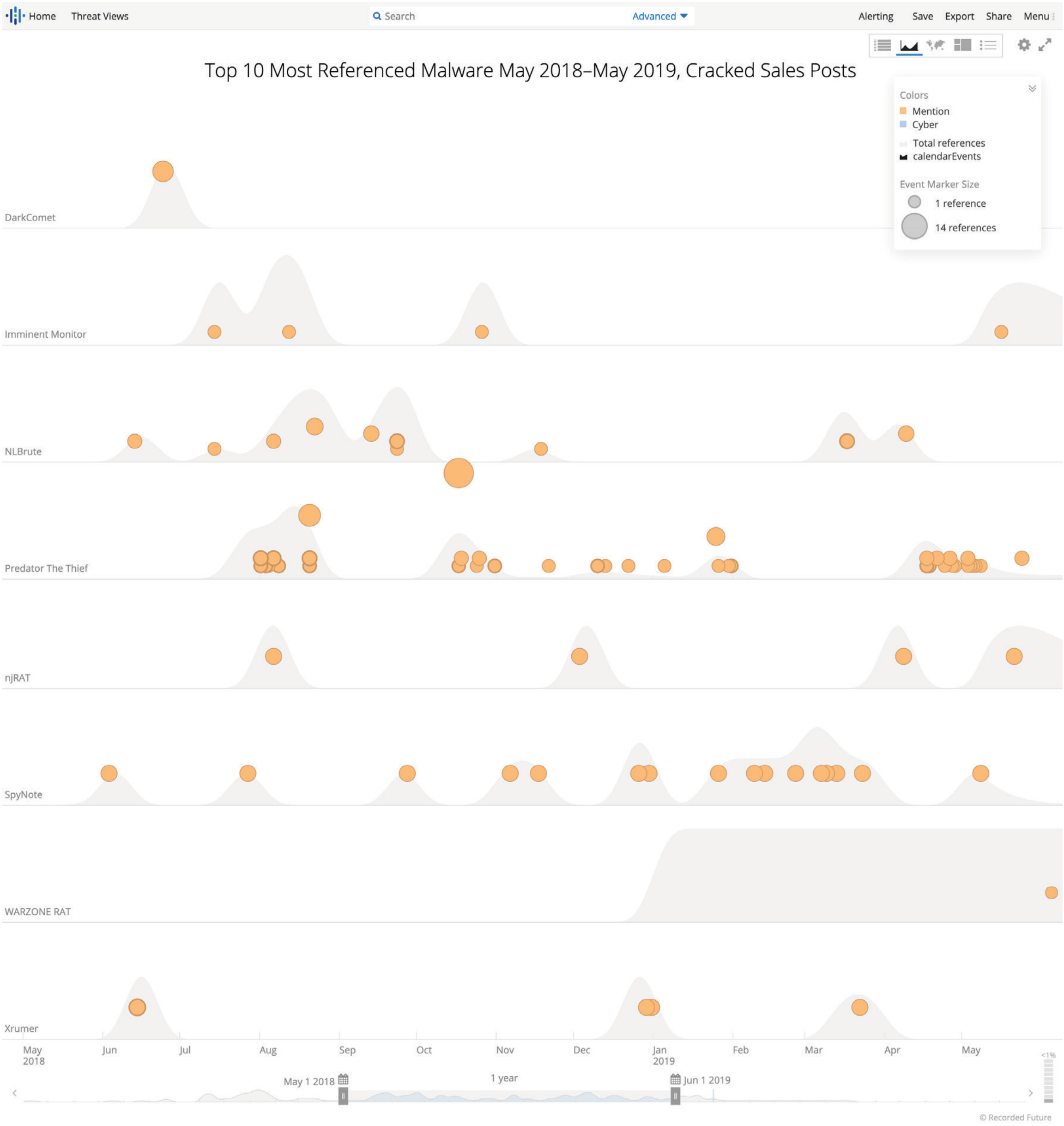
Posts in thread 232
First posting May 31 2018, 13:27
Most recent posting May 03 2019, 17:05

Didn't even know this was still being updated. Thanks.
Post 22 of 232 by Convo on Jun 11 2018, 10:47

Forum posts for two separate versions of njRAT. (Source: Recorded Future)

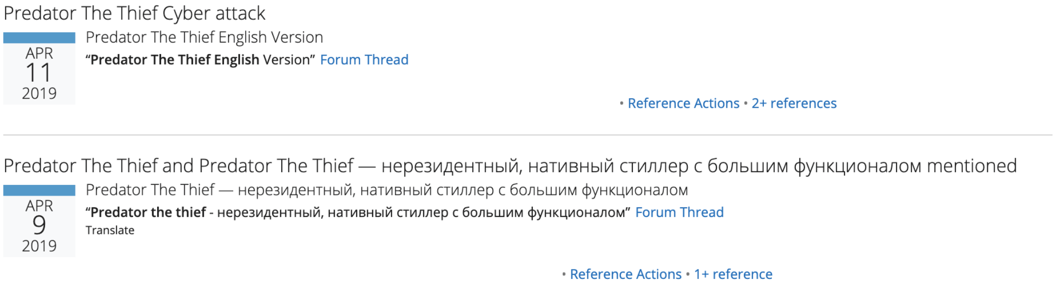
Distribution of Cracked Versions of Malware

A cracked version of malware, like a cracked version of software, is malware that has been altered to allow for possible unauthorized copying and utilization of previously proprietary programs, breaching the terms of service with the original vendor. Eight malware variants named in the top 10 within this report had been cracked and sold on an underground forum this past year. The two families of malware that had not been sold in cracked versions are njRAT (which is open-sourced and does not need to be cracked) and GandCrab.



Forum sales posts for cracked versions of the top 10 most referenced malware. (Source: Recorded Future)

According to our research, we assess with medium confidence that there were four primary drivers that caused chatter around a family of cracked malware to grow. First, a cracked variant of malware allowed more individuals to access the malware, especially if the malware was initially only sold on a closed forum or a forum with limited access. Second, vendors who crack malware with the intention of selling it had an incentive to advertise their malware on multiple forums, as cracking another forum member's malware can cause the new vendor to be banned from the initial forum. Third, altering malware to crack it, or altering the malware after it had been cracked, allowed vendors to tailor the additional functionality of the malware to suit audiences of different geographic regions. For example, multiple versions of Predator the Thief, an originally Russian malware family, had been cracked and altered in the past year to be tailored to an English audience.



Predator The Thief Cyber attack

APR 11 2019

Predator The Thief English Version

"**Predator The Thief English** Version" Forum Thread

• Reference Actions • 2+ references

Predator The Thief and Predator The Thief — нерезидентный, нативный стиллер с большим функционалом mentioned

APR 9 2019

Predator The Thief — нерезидентный, нативный стиллер с большим функционалом

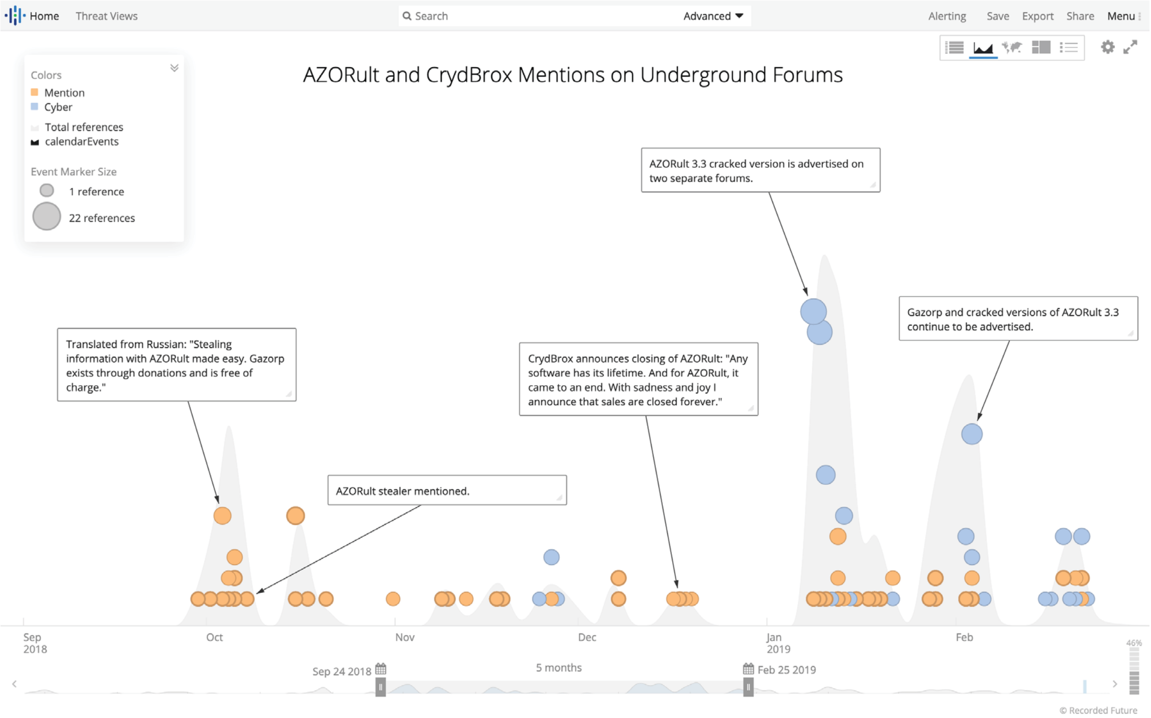
"**Predator the thief** - нерезидентный, нативный стиллер с большим функционалом" Forum Thread

Translate

• Reference Actions • 1+ reference

Forum sales post for the English version of Predator the Thief next to a forum sales post for a cracked version in the original Russian language. (Source: Recorded Future)

Finally, the cracked version of the software could cause the original vendor to update their code to make the tool more appealing than the cracked, now more readily available, previous version. For example, a builder for AZORult, named "Gazorp," was advertised on underground forums in September 2019 by an individual not endorsed by the original AZORult vendor. Gazorp created identical builds of AZORult 3.0, which was possible only because the source code for AZORult's admin panel had been leaked earlier, alongside an older, legitimate AZORult builder. On October 4, 2018, the original author of AZORult, CrydBrox, updated their version of the stealer. During September and October 2018, the number of references for AZORult were far higher than in previous and later months. December 2018 saw a dip in references — during this time, CrydBrox announced that they were no longer selling or updating AZORult. AZORult's reference count in January 2019 then spiked again, when the cracked version of AZORult 3.3 was released.



AZORult 3.3 cracked version is advertised on two separate forums.

Gazorp and cracked versions of AZORult 3.3 continue to be advertised.

Translated from Russian: "Stealing information with AZORult made easy. Gazorp exists through donations and is free of charge."

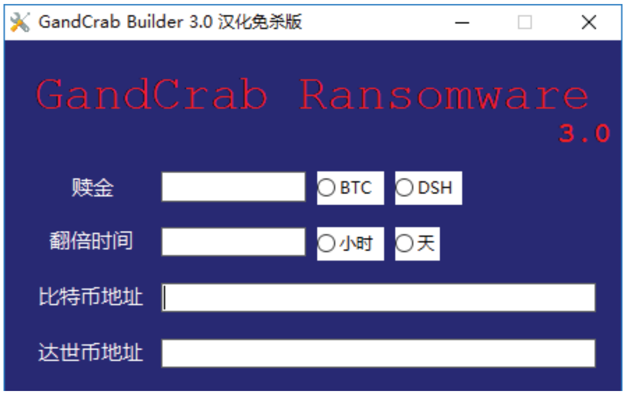
CrydBrox announces closing of AZORult: "Any software has its lifetime. And for AZORult, it came to an end. With sadness and joy I announce that sales are closed forever."

AZORult stealer mentioned.

Timeline of cracked versions and updates to AZORult from October 2018 to February 2019. (Source: Recorded Future)

Ultimately, cracked malware is detrimental for both the original malware developer and for potential victims, as the original malware developer loses control of both the malware and any profits based on its sale. Additionally, because more individuals use the malware, this results in additional versions of the malware with different functionality, which makes defending against or hunting for the malware more difficult.

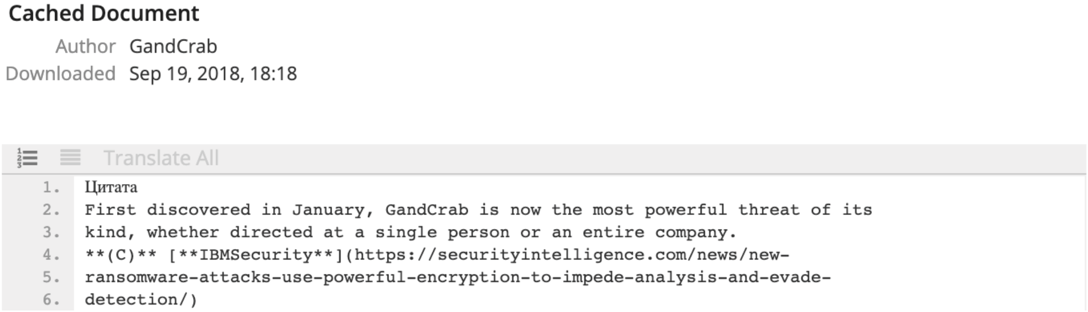
Of the 10 families of malware analyzed, the only families of proprietary malware still updated by the original author were GandCrab, Imminent Monitor, and WARZONE RAT (although the majority of WARZONE RAT and Imminent Monitor mentions on underground forums referenced cracked versions). While GandCrab has not yet been cracked, multiple vendors had attempted to sell their own ransomware under the GandCrab name. This grew the number of users who claimed to be using the malware, and provided incentives for the scammer selling the malware to put their sales post on multiple forums. For example, 360CN reported on a Chinese underground forum member selling a Chinese GandCrab ransomware builder. According to 360CN, the builder did create ransomware with the correct amount of ransom and Bitcoin address specified by a user, but also installed a cryptominer on the buyer's machine.



Fake GandCrab ransomware builder found on a Chinese language forum.

News Articles

Similarly to how cybersecurity blue teams and defenders of enterprise networks use news articles or security research as inspiration to strengthen defenses, cybercriminals use the same news articles or research as inspiration for how to breach defenses. In fact, almost all GandCrab posts on non-Russian forums were reposts of security news articles related to GandCrab updates, analysis reports on GandCrab, and decryptors for older versions of GandCrab. GandCrab also used news articles of their namesake malware to further advertise their product.


Cached Document

Author GandCrab

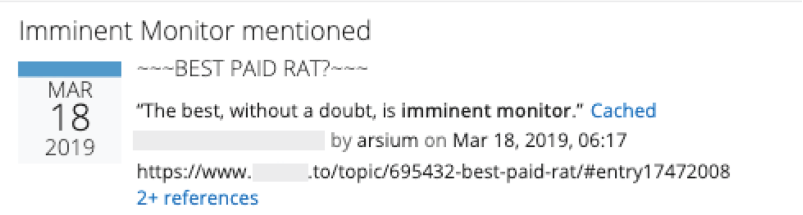
Downloaded Sep 19, 2018, 18:18

```
Цитата
First discovered in January, GandCrab is now the most powerful threat of its
kind, whether directed at a single person or an entire company.
**(C)** [**IBMSecurity**](https://securityintelligence.com/news/new-
ransomware-attacks-use-powerful-encryption-to-impede-analysis-and-evade-
detection/)
```

Recorded Future cached post of GandCrab using an IBM Security link to advertise their malware. (Source: Recorded Future)

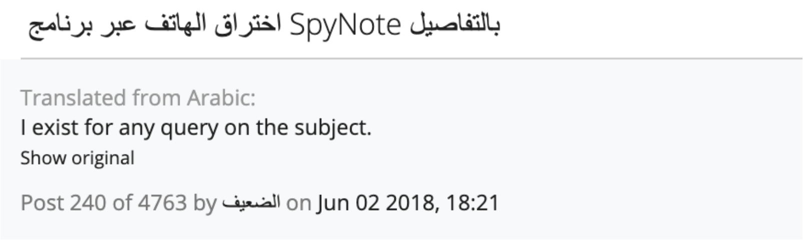
Customer Service and Community Engagement

A malware family usually did not have a significant number of mentions simply through a single vendor posting about the malware. Our data demonstrated that all of the 10 malware variants analyzed in this piece had an engaged set of underground community members. njRat, AZORult, Predator the Thief, SpyNote, NLBrute, Xrumer, DarkComet, Imminent Monitor, and WARZONE RAT all have tutorials readily available on YouTube, created by security researchers and hackers alike. These tutorials make setup easier for newer buyers, allowing them to follow a demonstration of how to set up the administrator panel, or how to infect another machine for "research purposes." In addition, buyers who used a specific malware family often became advocates for the malware by thanking the vendor publicly, posting a positive review of the vendor, or even posting about the malware on other forums or threads.



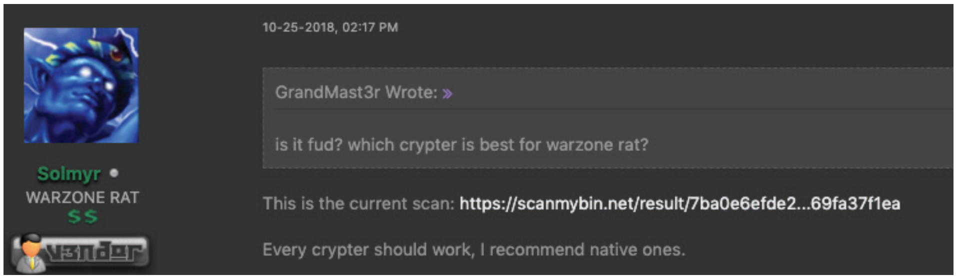
Imminent Monitor mentioned

MAR 18 2019

~~~BEST PAID RAT?~~~

"The best, without a doubt, is **imminent monitor**." Cached

[redacted] by arsium on Mar 18, 2019, 06:17

https://www.[redacted].to/topic/695432-best-paid-rat/#entry17472008

2+ references

Forum member posting about Imminent Monitor on a forum thread about good paid RATs. (Source: Recorded Future)

Because forum members could also post comments on the initial public sales thread, the vendor was also incentivized to provide customer service if a buyer posted a question.

Conversely, a majority of underground forums provided members with methods to report vendors of fake or faulty malware. This gave malware vendors an incentive to provide help to newer users or provide bug fixes and updates, while also allowing community members to ban less reputable vendors, whose posts would then either be deleted or die out.



اختراق الهاتف عبر برنامج SpyNote بالتفاصيل

Translated from Arabic:

I exist for any query on the subject.

Show original

Post 240 of 4763 by الضعيف on Jun 02 2018, 18:21

SpyNote vendor stating that they will answer any questions on their SpyNote post. (Source: Recorded Future)
~~~

Risk Mitigation: Is This a Risk to My Environment?

The ultimate question that an analyst has to address when conducting forum-related research is how a malware family discussed on an underground forum actually makes an impact on a defender's endpoint. In a few cases, malware advertised on underground forums will have little impact on a defender. For example, Xrumer is strictly a forum- or comment-based search engine optimization tool — while it can become a nuisance for any web application admin who has commenting enabled on their site, this tool is unlikely to do more damage than other tools specifically targeting web applications. In other cases, the malware is not effective without a delivery vehicle. For example, most RATs or ransomware require another vehicle of delivery, such as an exploit kit, phishing email, or brute-forced credentials, to install the malware on a victim host before it can be run. Additionally, many of the top 10 pieces of malware were advertised with crypters, as the vendors understood that their products could be easily detected with antivirus software.



10-25-2018, 02:17 PM

GrandMast3r Wrote: »

is it fud? which crypter is best for warzone rat?

This is the current scan: https://scanmybin.net/result/7ba0e6efde2...69fa37f1ea

Every crypter should work, I recommend native ones.

Solmyr, the vendor of WARZONE RAT, recommending that operators use a crypter to help customers' WARZONE RAT samples evade detection.

However, some of the malware has been known to be used in longer campaigns using more sophisticated malware. For example, NLBrute was used to create the initial infection vector for actors to deliver SamSam ransomware, and APT-C-36 was seen utilizing Imminent Monitor in February 2019.

Insikt Group assesses with medium confidence that a majority of the malware analyzed in this report can be classified as a low to moderate threat to a customer environment, and that due to the number of underground forum members sharing, deploying, and providing reviews about the malware, the malware is likely seen in the wild with high frequency.

To measure the number of samples deployed in the wild, Insikt Group created VirusTotal queries for samples that flagged specific antivirus names for the malware families in the table below, from March 2018 onwards. The following queries likely represent a fraction of the overall samples in the wild — this is due to the number of defenders that will use VirusTotal over a separate malware analysis engine (if utilizing one at all), as well as tendencies for antivirus companies to tag malware as "general" or "malicious" instead of by the name of the malware. Insikt Group also used Shodan and measured the number of potential targets for NLBrute (which is used for initial infection and is not dropped on a victim host) and certain GandCrab campaigns. Each hash likely represents a malware sample dropped on at least one victim host, adding up to a minimum number of 417,163 infections in the last year.

Malware	Query	Results
njRat	njRat samples submitted to VirusTotal after May 1, 2018	177,110 hashes
Predator the Thief	Predator the Thief samples submitted to VirusTotal after May 1, 2018	12,180 hashes
SpyNote	SpyNote android samples submitted to VirusTotal after May 1, 2018	113 hashes
AZORult	AZORult files submitted to VirusTotal after May 1, 2018	3,480 hashes
GandCrab	GandCrab samples submitted to VirusTotal after May 1, 2018	123,950 separate hashes
DarkComet	DarkComet samples submitted to VirusTotal after May 1, 2018	10,670 separate hashes
Imminent Monitor	Imminent Monitor samples submitted to VirusTotal after May 1, 2018	2,770 separate hashes
WARZONE RAT[2]	Ave Maria samples submitted to VirusTotal after May 1, 2018	2,500 separate hashes

Top 10 referenced malware and associated hash results on VirusTotal by AV detection name.

[2] Insikt Group assesses with high confidence that Ave Maria stealer is WARZONE RAT, based on previous reporting, C2 similarity, execution flow similarity, and Ave Maria RAT YARA rule matches on cracked WARZONE RAT samples found by Recorded Future. Additionally, samples from previous reporting on Ave Maria RAT found in the wild, as well as cracked versions of WARZONE RAT found on underground forums by Recorded Future, had a TLSH hashing score of 35, a score reserved for almost identical files.

As seen in the table in the "Network Defense Recommendations" section below, Insikt Group also separated the malware by unique delivery mechanism. In the last year, every malware family had at least one associated campaign, used by either a criminal group or a state actor.

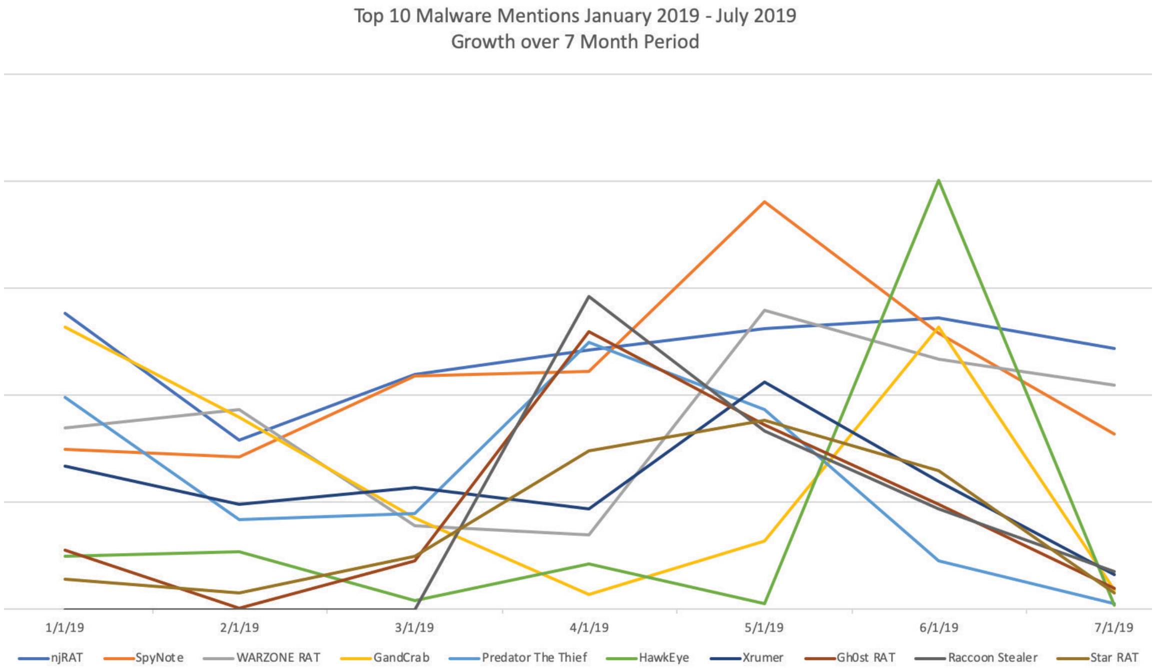
Outlook

Using a data-driven approach, Insikt Group has ascertained the most popular malware and malware categories in the past year so that companies may better triage their threats and delegate their security resources. A majority of these malware variants were created over a year prior to this report, and some tools are also dual-use or open source tools, greatly underscoring the importance of cooperation between the SOC and internal penetration testing teams to ensure that enterprises are protected both from commodity malware and tools regularly used by security researchers. Tracking the growth of malware mentions over time also gave our team more insight into the habits of malware vendors and buyers, and what particular activity on underground forums makes certain malware more successful than others.

While Insikt Group realizes that most mature security teams will already be defending against most of these top 10, Recorded Future recommends that smaller companies with growing teams use this report to establish a patching baseline off the malware and vulnerabilities mentioned in the "Network Defense Recommendations" below and throughout this report. By first defending against the highest-frequency attacks, security teams can then focus on the more mature, quieter threats that employ defensive evasion or longer-term persistence.

Finally, Insikt Group ascertains with high confidence that the top tools on underground forums will continue to change. While this research has exclusively focused on trends in the last year, forum activity in the last seven months suggests that new tools are emerging. While the six families of malware in the top 10 remain popular, spikes in activity surrounding newly emerging Raccoon Stealer and new versions of Hawkeye Keylogger (during April 2019 and June 2019 respectively) have occurred, as well as gradual increases in comments about Gh0st RAT (an open source RAT first created by Chinese developers in 2008) and Star RAT (another Chinese RAT whose source code has been widely shared on Chinese underground forums).

Insikt Group recommends that defenders continue to monitor the underground to find their new baseline of high-frequency, low-medium impact tools to defend against. If defenders have ascertained that they are consistently targeted by actors in specific geographic regions, or actors who would likely be active on forums of a certain language, Insikt Group further recommends that defenders focus on finding their baseline by monitoring the tools most referenced on those specific forums.



Most referenced malware mentions. (January 2019 to July 2019)

Network Defense Recommendations

Because most malware analyzed in this piece is not effective without a delivery vehicle, Insikt Group researchers separated the malware in the table below by delivery mechanism for campaigns using the malware reported on between 2018 and 2019 to ascertain vulnerabilities surrounding the malware. Insikt Group then found the vulnerabilities associated with the delivery mechanisms (see Appendix A).

Malware	Delivery Mechanisms
njRat	Malspam, Removable Drives
Predator the Thief	Malspam (CVE-2018-20250)
SpyNote	Sideloaded Application
AZORult	RIG EK, Fallout EK
NLBrute	Delivery Mechanism for Other Payloads via Brute-Forcing RDP
GandCrab	MySQLdb Scanning, RIG EK, Phishing, Magnitude EK, Grandsoft EK
Xrumer	Delivery Mechanism for Spam
DarkComet	Malspam, Phishing (CVE-2014-6352)
Imminent Monitor	Phishing (CVE-2017-11882), Spearphishing
WARZONE RAT	Phishing (CVE-2017-11882)

Top 10 malware and associated delivery mechanisms. (May 2018 to May 2019)

Editor's Note*: EK = Exploit Kit.*

Insikt Group recommends that organizations conduct the following measures outlined in this section:

- Prioritize patching within your organization for the vulnerabilities listed in Appendix A.
- Configure your intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and upon review, consider blocking — illicit connection attempts from known C2s related to the top 10 malware listed in this report.
- Configure your IDS or IPS to block connection requests related to open source security tools available via Metasploit, Kali Linux, or other offensive security tool repositories.

Appendix A — Vulnerabilities Utilized to Deliver Top 10 Referenced Malware

Vulnerabilities Utilized (May 2018 to May 2019)

RIG Exploit Kit

CVE-2018-8174, CVE-2018-4878, CVE-2015-2419, CVE-2016-0189, CVE-2016-0034, CVE-2015-5119, CVE-2016-4117, CVE-2018-8120, CVE-2015-8651, CVE-2018-15982, CVE-2017-0143, CVE-2017-10271, CVE-2017-5638

Fallout Exploit Kit

CVE-2018-8174, CVE-2018-4878, CVE-2018-15982

Magnitude Exploit Kit

CVE-2018-8174, CVE-2016-1019, CVE-2018-4878, CVE-2013-2551, CVE-2013-2643, CVE-2015-0311, CVE-2015-3113, CVE-2015-7645, CVE-2016-1015, CVE-2016-1016, CVE-2016-1017, CVE-2016-4117, CVE-2018-15982, CVE-2015-8651, CVE-2016-0189, CVE-2011-3402, CVE-2012-0507

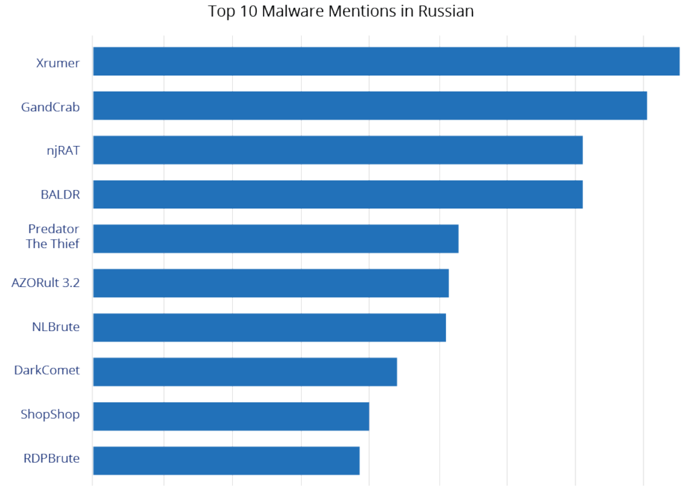
Grandsoft Exploit Kit

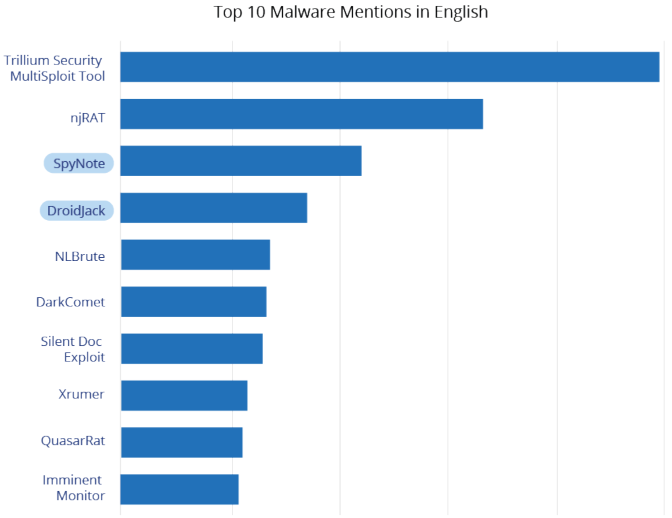
CVE-2016-0189, CVE-2018-8174, CVE-2018-4878, CVE-2018-15982

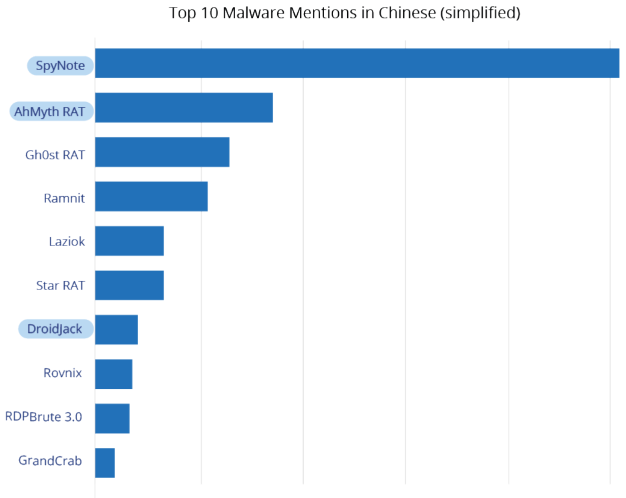
Phishing Campaigns

CVE-2018-20250, CVE-2017-11882, CVE-2014-6352

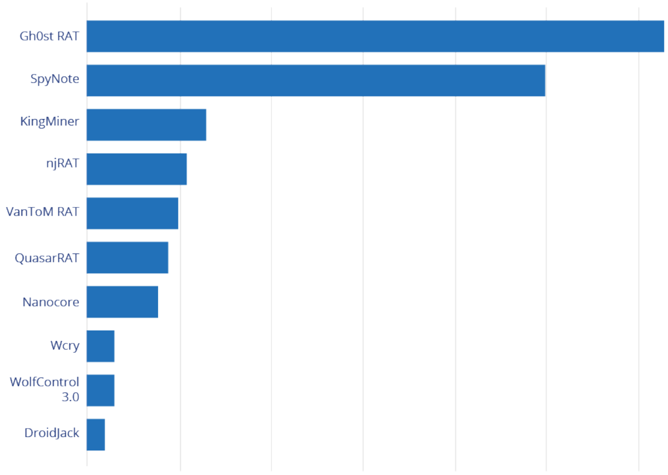
Appendix B — 2018 Malware Trend Analysis Graphs by Language



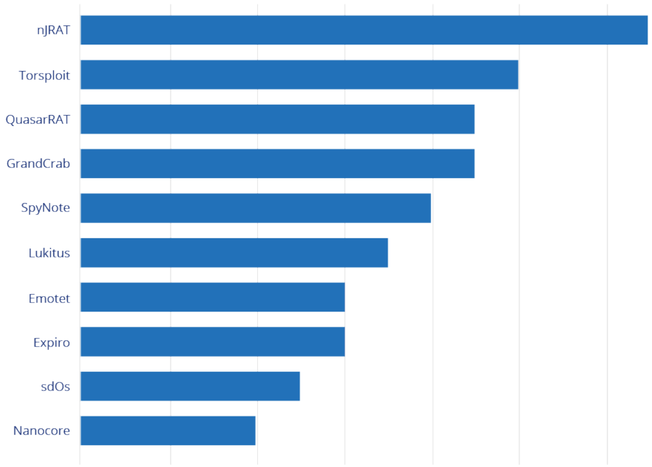




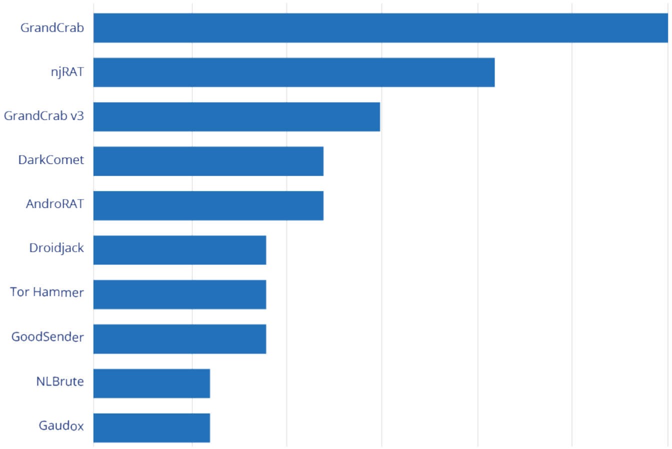
Top 10 Malware Mentions in Chinese (traditional)

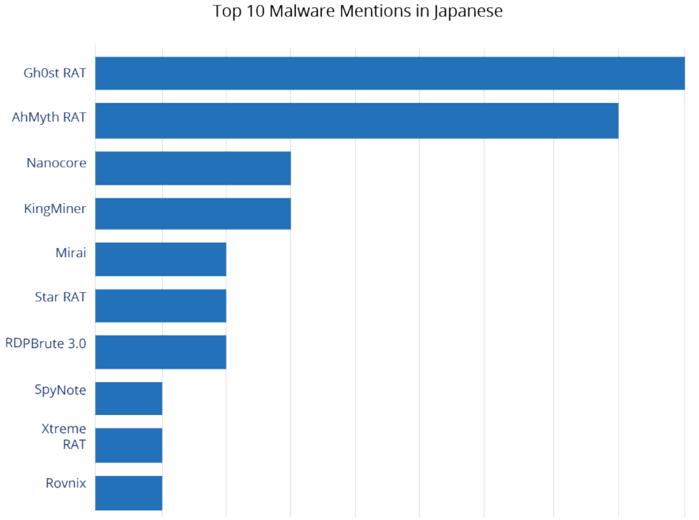


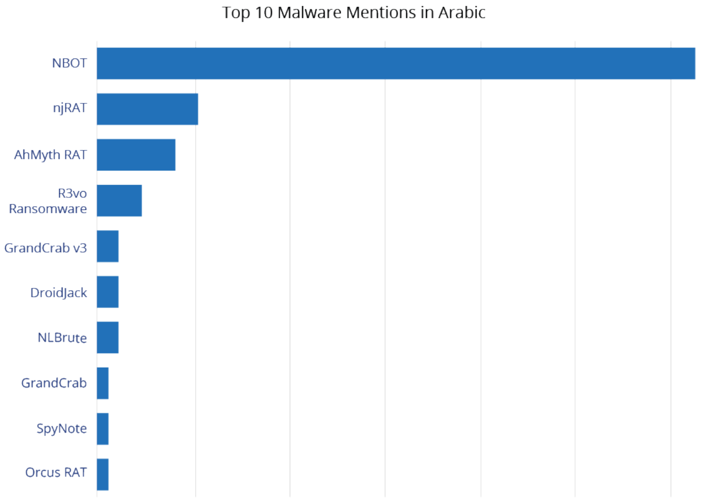
Top 10 Malware Mentions in Spanish



Top 10 Malware Mentions in Farsi







About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.