Bestsellers in the Underground Economy
Measuring Malware Popularity by Forum
Winnona
Threat Intelligence Researcher @ Recorded Future

Fellow @ Harvard Kennedy School Belfer Center Cyber Project
Organizer @ Boston Security Meetup
Featured in Tribe of Hackers

I talk about China and the Internet sometimes

🐦 @__winn
The thoughts are my own, the gifs are not.

Paper available at: recordedfuture.com/measuring-malware-popularity
Why Monitor Criminal / Underground Forums?

- Company information in data dumps
- Leaks and announcements of illegal activity
- Monitoring shifts in targeting and tactics before they are utilized
Monitoring Shifting Tools - so many questions

- What are the most talked about families of malware on underground forums?
Monitoring Shifting Tools - so many questions

- What are the most talked about families of malware on underground forums?

- Is ransomware really becoming the new type of malware people are gravitating to?
Monitoring Shifting Tools - so many questions

- What are the most talked about families of malware on underground forums?
- Is ransomware really becoming the new type of malware people are gravitating to?
- What factors are correlated to a malware’s popularity and how does this change over time?
How can we translate underground criminal activity (primarily CTI) into actionable intelligence that informs pentesters and defenders?
“Wow do u look at hackers on the dark web”
Deep/Dark Web is not an accurate focus.

Hackers and criminals conduct criminal activity everywhere, including:

- 3rd Party Chat Applications / Social Media
- Forums openly available on the open Internet
- Tor / I2P
- Mail / In person transactions
Ecosystem of Vendors & Buyers
Discussions and questions

Ghee Buttersnaps Wrote: »

Are you offering vouch copies?

jepko Wrote: »

I will make a detailed review if you provide a copy.

Vouch copies sent to both of you guys!
Thank you for your interest!

Mr.Ransom Wrote: »

no lifetime packages? seems interesting

I plan to run it for a long time. Lifetime package would make it hard to sustain in a long run.
Research Scope:

Analysing 3.9 million posts over the last year that mention a name or category of malware to find the most referenced types/families.
This research encompasses all of the following sources available on the Internet:

- 3rd Party Chat Applications / Social Media
- Forums openly available on the open Internet
- Tor / I2P
Methodology

61 malware categories
101,124 malware names

(created over the course of 5+ years with Recorded Future)
Definition of malware used = “operational pieces of code used to conduct illegal activity”.

- Reposts of news articles and security research

- Spam posting (some required manual removal)
Gleaning Insight from Data

- Malware Mentions Overall
- Malware Raw Mentions by Language
- Correlations between Forum / Real World events and Growth in Malware Mentions
Malware Mentions
Overall
Category vs. Family Results

Top Malware Categories in the Last Year (May 2018 - May 2019)

- Ransomware
- Crypter
- Trojan
- WebShell
- Remote Access Trojan
- Adware
- Computer virus
- FUD crypter
- Exploit Kit
- Rootkit
Category vs. Family Results

Top 10 Malware Mentions May 2018 - May 2019

njRAT
Predator The Thief
SpyNote
azorult
NLBrute
GandCrab
Xrumer
DarkComet
Imminent Monitor
WARZONE RAT
Category vs. Family Results

Top 10 Malware Mentions May 2018 - May 2019

- njRAT
- Predator The Thief
- SpyNote
- AZORult
- NLBrute
- GandCrab
- Xrumer
- DarkComet
- Imminent Monitor
- WARZONE RAT
Prevalence of Branded Ransomware (or lack thereof)

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6:</td>
<td>30:</td>
<td>51:</td>
<td>73:</td>
</tr>
<tr>
<td>GandCrab</td>
<td>Wannacry</td>
<td>Cryptolocker</td>
<td>Princess Locker</td>
</tr>
<tr>
<td>84:</td>
<td>88:</td>
<td>110:</td>
<td>124:</td>
</tr>
<tr>
<td>Petya</td>
<td>NotPetya</td>
<td>Relock</td>
<td>Saturn Ransomware</td>
</tr>
<tr>
<td>125:</td>
<td>133:</td>
<td>144:</td>
<td></td>
</tr>
<tr>
<td>Samsam</td>
<td>Ryuk Ransomware</td>
<td>Rapid Ransomware</td>
<td></td>
</tr>
</tbody>
</table>

*Table 1: Named Ransomware within the dataset in the top 150*
Hi, we're a fairly big vendor on Dream market and we're looking to expand our business. We are looking for Ransomware as a Service to deploy in Europe. We have heard many stories about a forum where you are able to find GandCrab, a specific RaaS, but we are open to find any ransomware as long as they're good and reliable. Can someone help us out? We'll send 100gr MDMA for free and some cocaine to the person who is able to hook us up with GandCrab and 50gr MDMA for free to whoever is able to hook us up with a proper and just as good alternative. Thanks :)

Post 1 of 1 by HelloFresh on Dec 04 2018, 05:37
Raw Malware Mentions by Language
Why split out language?

Hacking communities in the different countries have completely different cultures and origins, and languages.
Why split out language?

Hacking communities in the different countries have completely different cultures and origins, and languages.

Does this shape their advertised malware and targets?
Different Tools and Targets on Different Forums (Mobile Malware?)

Top 10 Malware Mentions in Chinese (simplified)
Different Tools and Targets on Different Forums (Mobile Malware?)
Different Tools and Targets on Different Forums (Mobile Malware?)

Top 10 Malware Mentions in Russian

- Xrumer
- GandCrab
- njRAT
- BALDR
- Predator The Thief
- AZORult 3.2
- NLBrute
- DarkComet
- ShopShop
- RDPBrute
Overarching Similarities Across Languages

- Old malware (3+ years old)
- Dual use tools
- Forum specific malware
- GandCrab (rip)
Correlations between Malware and Real Life
Top 10 Malware Mentions May 2018 - May 2019

njRAT
Predator The Thief
SpyNote
azorult
NLBrute
GandCrab
Xrumer
DarkComet
Imminent Monitor
WARZONE RAT
Types of Growth

Top 10 Malware Mentions May 2018 - May 2019
Growth over 12 Month Period
3 Correlated Events

- Being a good vendor
- The sale of malware sets
- Distribution of cracked malware versions
Being a Good Malware Vendor

- Advertised updates
- Real world news articles
- Community engagement / customer service

Cached Document

Author GandCrab
Downloaded Sep 19, 2018, 18:18

1. First discovered in January, GandCrab is now the most powerful threat of its kind, whether directed at a single person or an entire company.

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. Added **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

Previous 50  Next 50

Show original

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

Download Links:

1. BasicLocker/shell-locker ransomware
   - Full source
   - Skiddy ScreenLocker
   Download:

2. NxRansomware
   - Full source
   - Full ASP Panel source
   Download:

3. HiddenTear
   - Full source
   - Coded by UtkuSen as opensource ransomware.
   Download:

4. MyLittleRansomware
   - Full source
   - RSA (uses Private/Public key)
   Download:

[X] WARZONE CRYPTER [X] Dedicated Native Crypter for WARZONE RAT

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

MAY 30

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

*Stealing information with AZORult made easy. Gazorp exists through donations and is free of charge.*

CrydBlox Updates AZORult to v3.3** UPD: v3.3
** [x] Added collection from wallets: BitcoinGold, electrumG, bitcoin (electrumshop), bitcore, Exodus Eden [x]
*Improved and improved collection from all other cryptocurrency wallets [+] Fixed and improved loader, now even batch files can be loaded, they will be executed without errors [+] Runtime cleaned, average cpu usage increased [+] Administrator load is slightly reduced*

AZORult 3.3 Cracked version is advertised on 2 separate forums.

CrydBlox 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.”

Gazorp and cracked versions of AZORult 3.3 continue to be advertised.
Is this actually a risk?
Lower threat, higher frequency

- Ineffective without a delivery vehicle, age, antivirus rules exist.
- Some cases, jumping off point for very high impact
  - NLBrute & SamSam
  - Imminent Monitor & APT-C-36
- Every top 10 family has been reported on as seen in the wild at least once since May 2018.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Query:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Results:</td>
<td>177,110 hashes</td>
<td>12,180 hashes</td>
<td>113 hashes</td>
<td>3,480 hashes</td>
</tr>
<tr>
<td>GandCrab</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DarkComet</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Imminent Monitor</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WARZONE RAT</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ave Maria</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GandCrab samples submitted to VirusTotal after 2018-05-01</td>
<td>123,950 separate hashes</td>
<td>10,670 separate hashes</td>
<td>2770 separate hashes</td>
<td>2500 separate hashes</td>
</tr>
</tbody>
</table>
In Conclusion...

Landscape will change, monitoring is necessary
Landscape will change, monitoring is necessary

Dual use tools:
Cooperation between the SOC and internal penetration testing teams are essential
In Conclusion...

Landscape will change, monitoring is necessary.

Dual use tools: Cooperation between the SOC and internal penetration testing teams are essential.

Finding baselines against different actor sets is important for enterprises targeted by specific groups.
Landscape will change, monitoring is necessary

Dual use tools: Cooperation between the SOC and internal penetration testing teams are essential

Finding baselines against different actor sets is important for enterprises targeted by specific groups.

Baseline for Patching
How can we translate underground criminal activity (primarily CTI) into actionable intelligence that informs pentesters and defenders?
How can we translate underground criminal activity (primarily CTI) into actionable intelligence that informs pentesters and defenders?

most commonly discussed malware, -> delivery vehicles ->

prioritizing patching against the vulnerabilities those delivery vehicles exploit.
Thank you!

recordedfuture.com/measuring-malware-popularity

winnona@recordedfuture.com

@_winn