ThreatCloud Intelligence Analysis:

Tales from the Crypter: Thwarting Malware Obfuscation with Threat Emulation

20 Jan 2013

Check Point Malware Research Group

Summary

Malware writers employ a variety of specialized obfuscation techniques to render known malware invisible to existing antivirus defenses. These techniques, known as “crypting,” enable malware writers to create unknown variants of proven, highly effective malware that evade AV detection and extend the reach of existing bot infrastructure.

Check Point Threat Emulation recently demonstrated that not all defenses are so easily evaded when it detected and blocked a crypted and previously unknown malware variant designed to deliver the DarkComet remote administration tool (RAT). Although this sample was able to evade most AV solutions, Threat Emulation was able to reveal it and additional investigation by our research team traced it to a malware campaign that has been detected at work in Europe and Latin America.

In addition to detecting and blocking this dangerous malware through the ThreatCloud network, this catch by Threat Emulation highlights the inner workings of the family of advanced attacks that are changing both the threat landscape, and the range of solutions that security managers need in order to defend their networks and their data.

Detailed Analysis

1. Intercepting a suspicious attachment

On December 31, 2013, Check Point ThreatCloud received an alert triggered by a Threat Emulation detection in a customer network. At the time of detection, the malware sample was unknown to the VirusTotal community and was able to pass numerous different antivirus engines with no detections. (VirusTotal is a Google-owned service that analyzes suspicious files and URLs and maintains a malware database that is shared back to the research community.)

The malware was sent by email from a fake Gmail address with the subject “PROFORMA INVOICE”, appearing to present a previously discussed possible purchase deal from a seller. The email included an attachment named ‘*PROFORMA_INVOICE.rar*’, which is a valid extractable RAR archive containing an executable file. Unlike attacks which exploit an OS or application vulnerability, this malware simply needs the end-user to run the executable once extracted from the RAR file.

Threat Emulation intercepted the attachment, extracted its contents, and attempted to open it in a controlled emulation environment, a process also referred to as ‘malware sandboxing.’ During emulation, it was detected that the file exhibited multiple suspicious activities when executed, including creating additional processes, writing suspicious files, and registering for system-wide notifications.

Based on these emulation results, this sample was forwarded for further analysis with Check Point Malware Research Group, which extracted the malicious payload and undertook additional analysis.

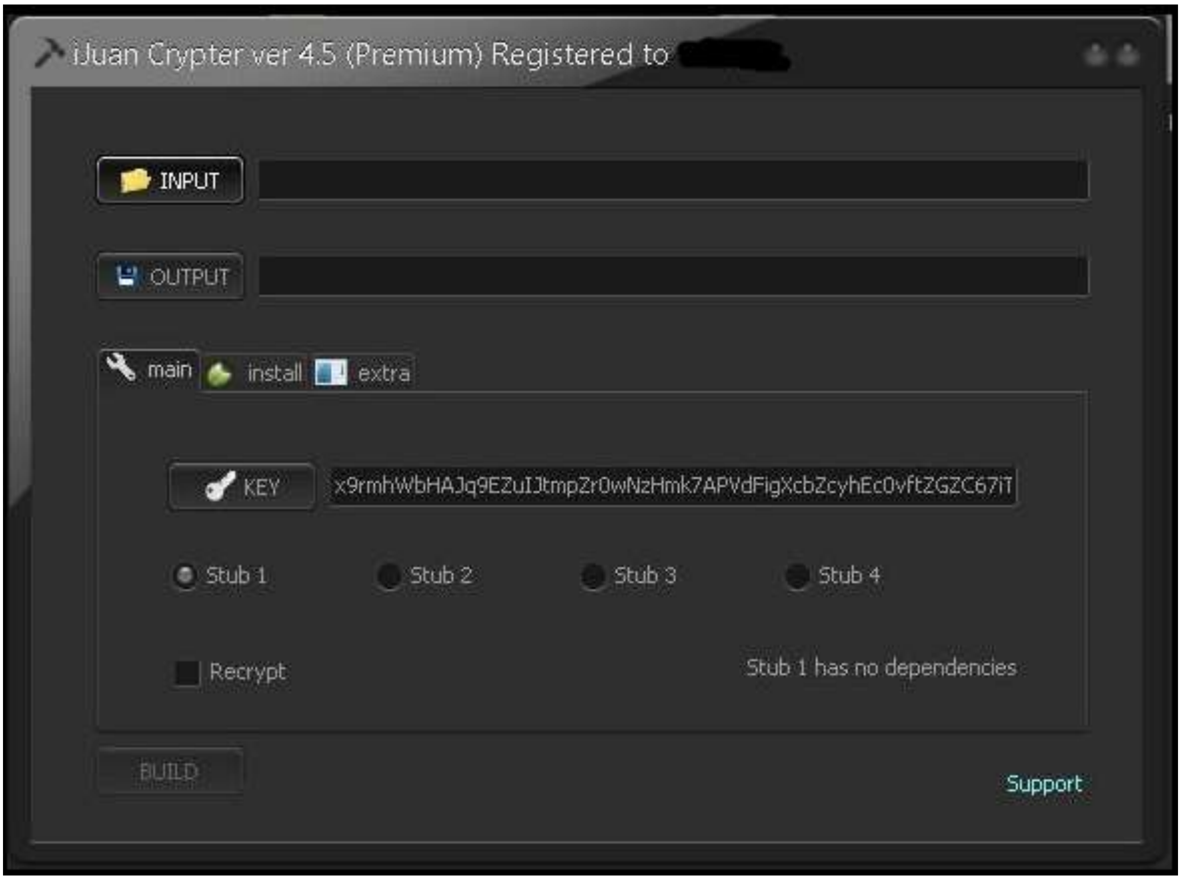
Analysis revealed that the executable contained an obfuscated version of the DarkComet RAT. DarkComet is a freely available remote administration tool (RAT), with useful abilities such as keylogging, screen captures, file transfers and more. When used maliciously, DarkComet can essentially turn any computer into a fully-featured bot, and this is, in fact, the primary notorious use for this software, as we often see evidence of DarkComet malware campaigns.

In its plain, non-obfuscated form DarkComet is detected by the majority of AV products.

2. ‘Crypter’ services make a business of antivirus evasion

In order to bypass detection by AV software, modern malware authors maintain and use specialized obfuscation tools called “crypters.” Technically classified as a Portable Executable (PE) Packer, and not to be confused with encrypting ransomware such as Cryptolocker, crypters like this sample disguise executables through the use of various encryption and encoding schemes, cleverly combined and recombined, often more than once. To verify that their variants are undetected, malware authors avoid online AV scanning platforms such as VirusTotal and others which share samples with AV vendors, and instead utilize ‘private’ services such as razorscanner, vscan (aka NoVirusThanks) and chk4me. PE Packers and other ‘crypters’ are classified by hacker communities as UD (UnDetectable) or FUD (Fully UnDetectable) according to their success at evading antivirus detection.

In the case of our detected sample, an embedded PDB string gave away that it was by the iJuan Crypter, which is available online both as a free (UD) version as well as a premium (FUD) purchase option. The fact that even malware writers are experimenting with the ‘freemium’ pricing model offers yet another example of the sophistication of the underground malware economy.



iJuan Crypter ver 4.5 (Premium) Registered to [redacted]

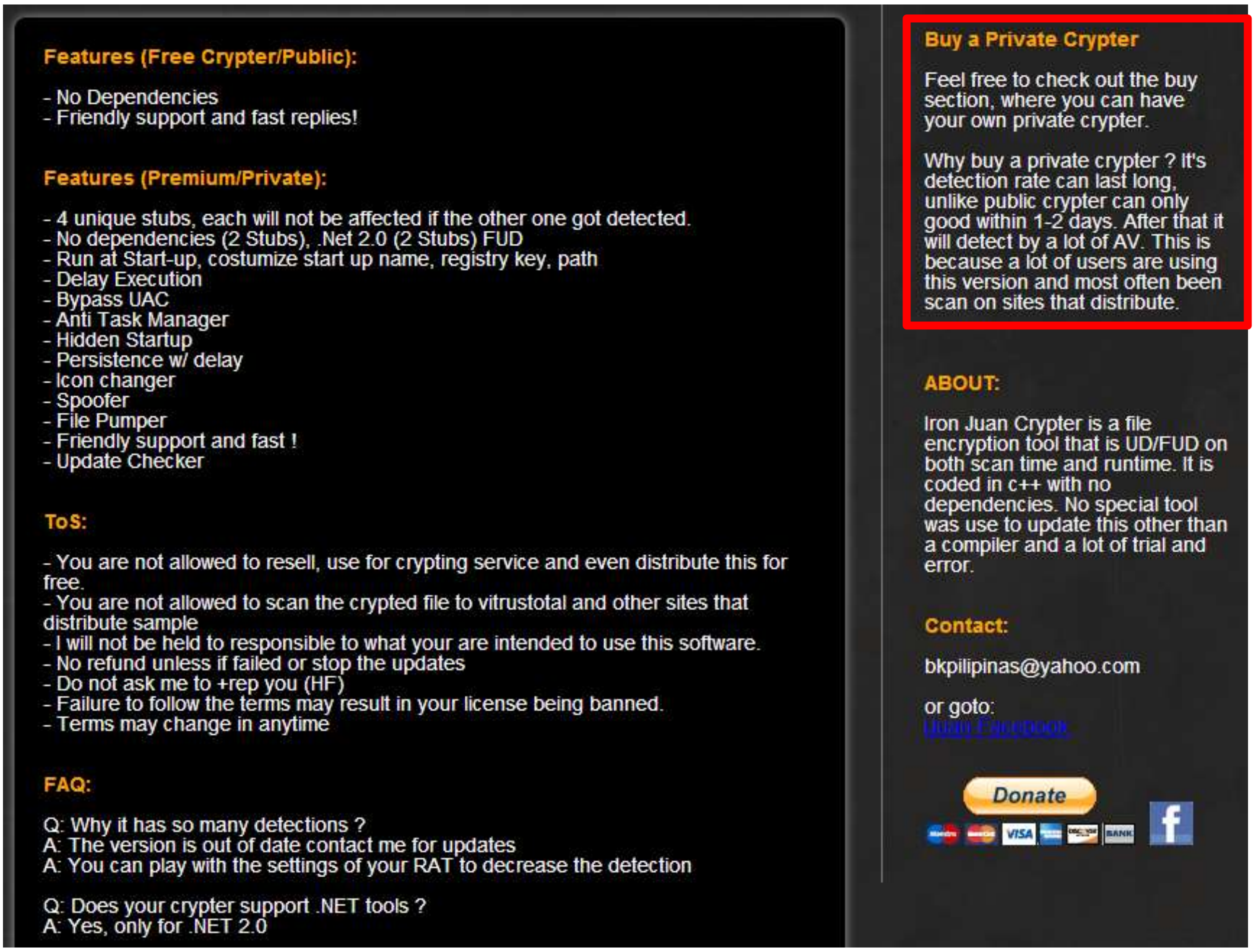
KEY: x9rmhWbHAJq9EZuIJtmpZr0wNzHmk7APVdFigXcbZcyhEc0vftZGZC67iT

● Stub 1 ○ Stub 2 ○ Stub 3 ○ Stub 4

□ Recrypt

Stub 1 has no dependencies

It may be surprising to some to read how the crypter author (nicknamed ‘Iron Juan’ but otherwise anonymous) boasts about the ability of his ‘crypting’ software to evade antivirus software, in obvious disregard for the potentially criminal intent of the users and buyers.



Features (Free Crypter/Public):

- No Dependencies
- Friendly support and fast replies!

Features (Premium/Private):

- 4 unique stubs, each will not be affected if the other one got detected.
- No dependencies (2 Stubs), .Net 2.0 (2 Stubs) FUD
- Run at Start-up, costumize start up name, registry key, path
- Delay Execution
- Bypass UAC
- Anti Task Manager
- Hidden Startup
- Persistence w/ delay
- Icon changer
- Spoofer
- File Pumper
- Friendly support and fast !
- Update Checker

ToS:

- You are not allowed to resell, use for crypting service and even distribute this for free.
- You are not allowed to scan the crypted file to vitrustotal and other sites that distribute sample
- I will not be held to responsible to what your are intended to use this software.
- No refund unless if failed or stop the updates
- Do not ask me to +rep you (HF)
- Failure to follow the terms may result in your license being banned.
- Terms may change in anytime

FAQ:

Q: Why it has so many detections ?
A: The version is out of date contact me for updates
A: You can play with the settings of your RAT to decrease the detection

Q: Does your crypter support .NET tools ?
A: Yes, only for .NET 2.0

Buy a Private Crypter

Feel free to check out the buy section, where you can have your own private crypter.

Why buy a private crypter ? It's detection rate can last long, unlike public crypter can only good within 1-2 days. After that it will detect by a lot of AV. This is because a lot of users are using this version and most often been scan on sites that distribute.

ABOUT:

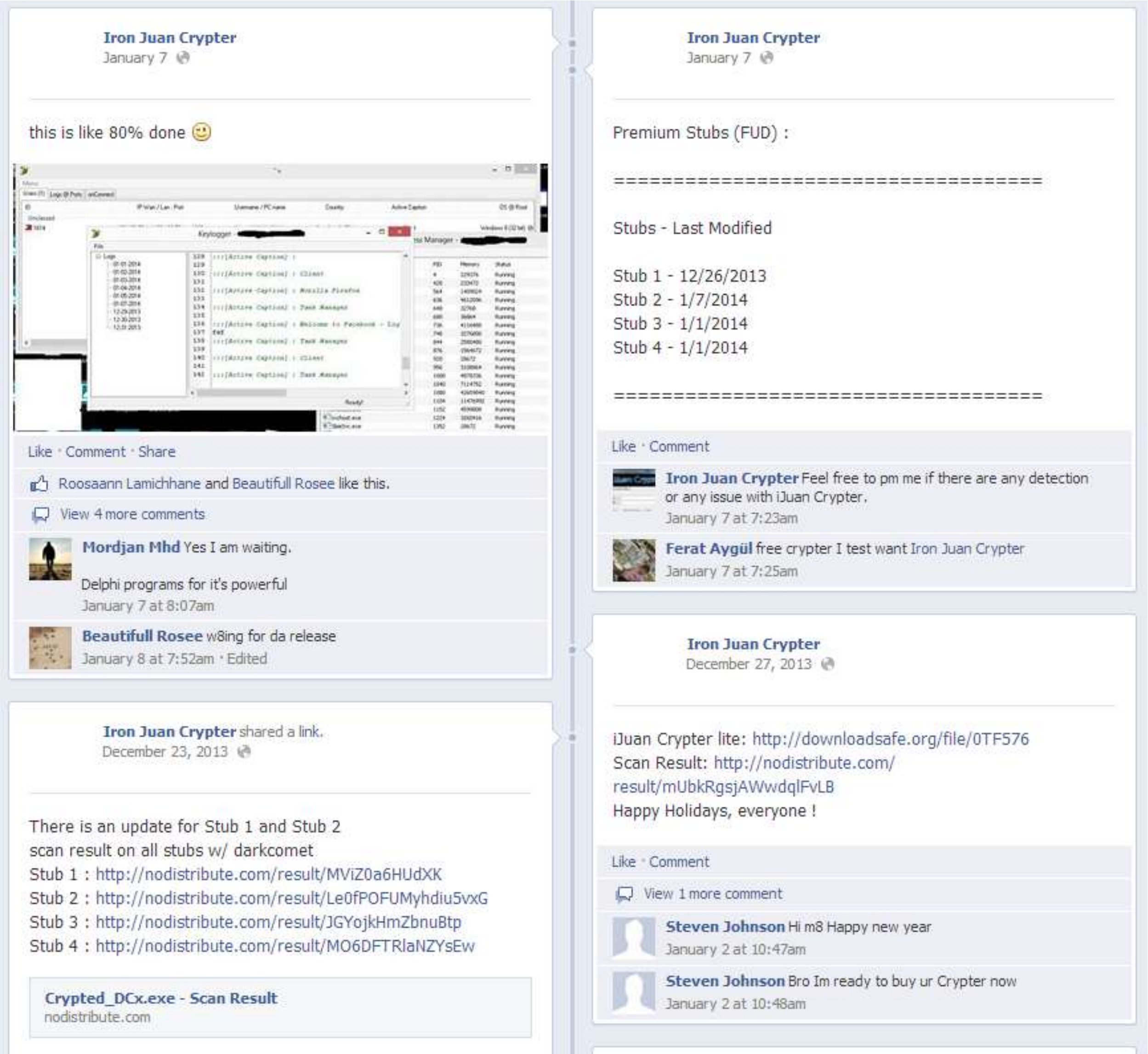
Iron Juan Crypter is a file encryption tool that is UD/FUD on both scan time and runtime. It is coded in c++ with no dependencies. No special tool was use to update this other than a compiler and a lot of trial and error.

Contact:

bkpilipinas@yahoo.com

or goto:
Juan Facebook

The ‘Iron Juan Crypter’ even has a Facebook page and YouTube channel, where the author describes and demonstrates his development progress across new versions, showing current detections to the enthusiastic and appreciative audience. (As with most sites in the underground malware community, average users are advised to exercise extreme caution when visiting any sites dedicated to buying, selling, trading and developing malware.)



Iron Juan Crypter
January 7

this is like 80% done 🙂

Like · Comment · Share

Roosaann Lamichhane and Beautifull Rosee like this.

View 4 more comments

Mordjan Mhd Yes I am waiting.

Delphi programs for it's powerful
January 7 at 8:07am

Beautifull Rosee w8ing for da release
January 8 at 7:52am · Edited

Iron Juan Crypter shared a link.
December 23, 2013

There is an update for Stub 1 and Stub 2
scan result on all stubs w/ darkcomet
Stub 1 : http://nodistribute.com/result/MViZ0a6HUdXK
Stub 2 : http://nodistribute.com/result/Le0fPOFUMyhdiu5vxG
Stub 3 : http://nodistribute.com/result/JGYojkHmZbnuBtp
Stub 4 : http://nodistribute.com/result/MO6DFTRlaNZYsEw

Crypted_DCx.exe - Scan Result
nodistribute.com

Iron Juan Crypter
January 7

Premium Stubs (FUD) :

====================================

Stubs - Last Modified

Stub 1 - 12/26/2013
Stub 2 - 1/7/2014
Stub 3 - 1/1/2014
Stub 4 - 1/1/2014

====================================

Like · Comment

Iron Juan Crypter Feel free to pm me if there are any detection or any issue with iJuan Crypter.
January 7 at 7:23am

Ferat Aygül free crypter I test want Iron Juan Crypter
January 7 at 7:25am

Iron Juan Crypter
December 27, 2013

iJuan Crypter lite: http://downloadsafe.org/file/0TF576
Scan Result: http://nodistribute.com/result/mUbkRgsjAWwdqlFvLB
Happy Holidays, everyone !

Like · Comment

View 1 more comment

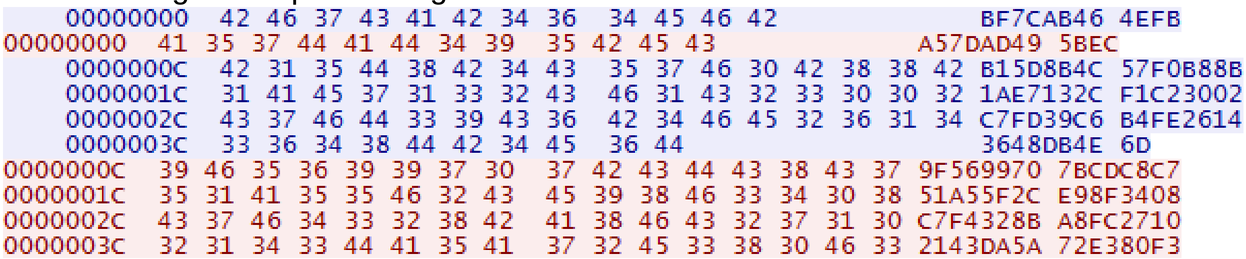
Steven Johnson Hi m8 Happy new year
January 2 at 10:47am

Steven Johnson Bro Im ready to buy ur Crypter now
January 2 at 10:48am

3. Uncovering the campaign

Once executed, the malware attempts to communicate with its hard-coded command and control (C&C) server at: ***roland1926.no-ip.biz:1604***

The following is sample traffic generated in our lab:



```
    00000000  42 46 37 43 41 42 34 36  34 45 46 42             BF7CAB46 4EFB
00000000  41 35 37 44 41 44 34 39  35 42 45 43             A57DAD49 5BEC
    0000000C  42 31 35 44 38 42 34 43  35 37 46 30 42 38 38 42 B15D8B4C 57F0B88B
    0000001C  31 41 45 37 31 33 32 43  46 31 43 32 33 30 30 32 1AE7132C F1C23002
    0000002C  43 37 46 44 33 39 43 36  42 34 46 45 32 36 31 34 C7FD39C6 B4FE2614
    0000003C  33 36 34 38 44 42 34 45  36 44                   3648DB4E 6D
0000000C  39 46 35 36 39 39 37 30  37 42 43 44 43 38 43 37 9F569970 7BCDC8C7
0000001C  35 31 41 35 35 46 32 43  45 39 38 46 33 34 30 38 51A55F2C E98F3408
0000002C  43 37 46 34 33 32 38 42  41 38 46 43 32 37 31 30 C7F4328B A8FC2710
0000003C  32 31 34 33 44 41 35 41  37 32 45 33 38 30 46 33 2143DA5A 72E380F3
```

Both the port and the communication pattern are highly indicative of DarkComet traffic, encrypted via a custom password RC4 algorithm, submitting victim data to campaign operators.

Less than a week after the initial detection, we received a second Threat Emulation alert for a similar detection in a different country. Performing a similar analysis has revealed it to be a differently obfuscated version of the same DarkComet payload and communicating to the same C&C server, which together indicate that these two distinct detections – one in Europe and the other in Latin America – are in fact part of the same campaign.

Protecting your organization from this type of attack

All Organizations

In order to reduce the chance of infection from this kind of malware, organizations should educate users not to open unexpected or suspicious attachments from external email addresses.

Check Point Customers

Customers who have enabled the Antivirus and Anti-Bot Blades on their Check Point gateways automatically received updated detections for these newly detected variants through ThreatCloud. For additional protection against previously undetected malware, customers should consider enabling Threat Emulation as a public or private cloud service.

Non-Check Point Customers

Non-Check Point Customers should monitor for outbound communication to *roland1926.no-ip.biz:1604* and take action to remediate infected clients.

Appendix

Hashes for detected malware are:

MD5:

```
fc2576a2883de7ed3f30b1fcbf937e38
b61b771c4b80c9ba8d6bba4d908fe9e5
f88093bea5abd4e8d859cf179d6e684e
```

SHA1:

```
d0afdbefa942b0f98c6a786afabedfc1cd5fedf8
90ac55fd5cb55a664b49622d8aedf64ad69c522d
7bc49c4a1801b5d04b54c63638534df7ddf13da1
```