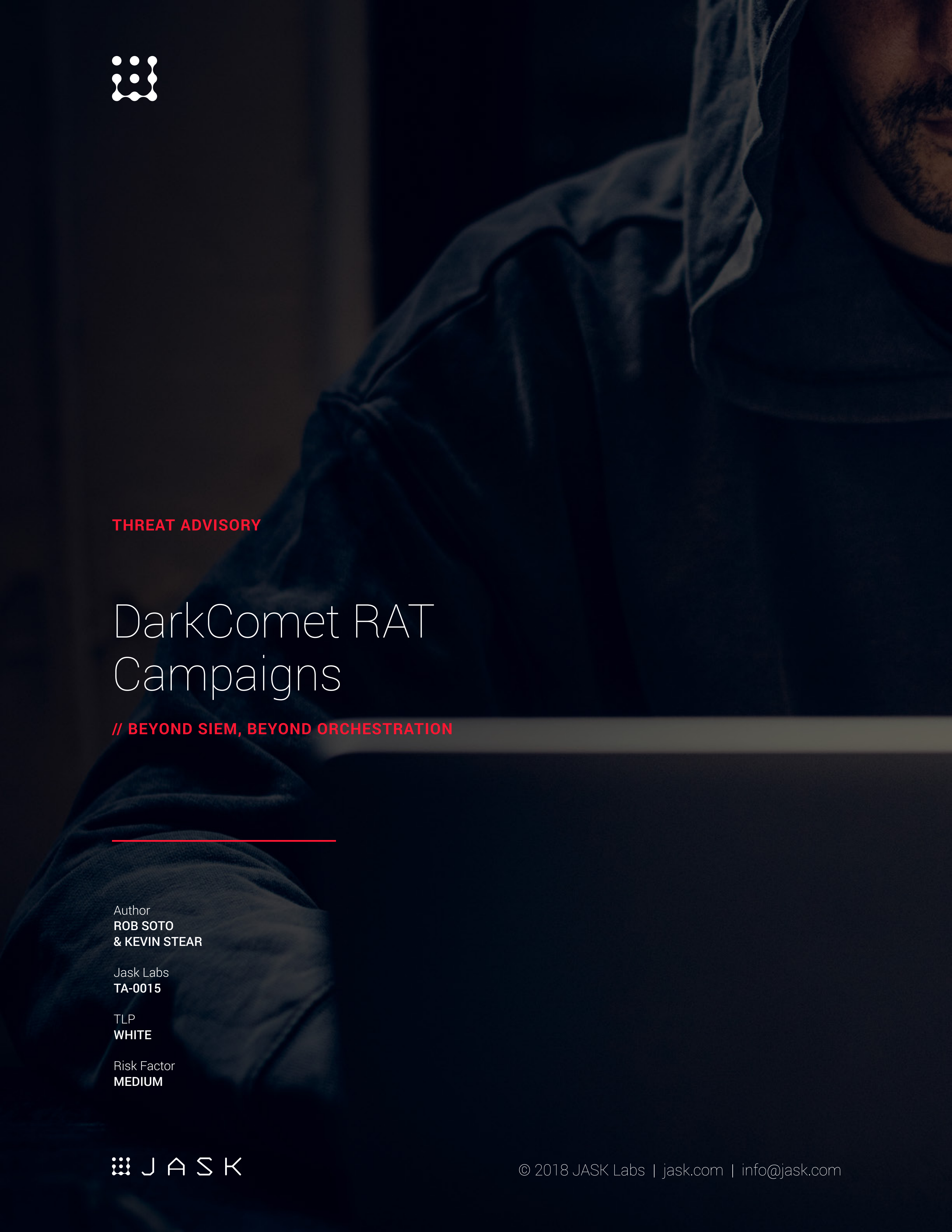


THREAT ADVISORY

DarkComet RAT Campaigns

// BEYOND SIEM, BEYOND ORCHESTRATION

Author
**ROB SOTO
& KEVIN STEAR**

Jask Labs
TA-0015

TLP
WHITE

Risk Factor
MEDIUM

THREAT ADVISORY

DarkComet RAT Campaigns

Author
ROB SOTO
& KEVIN STEAR

Jask Labs
TA-0015

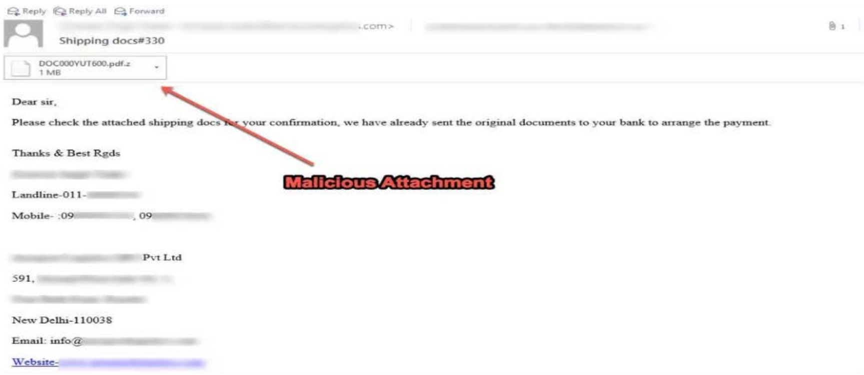
TLP
WHITE

Risk Factor
MEDIUM

Overview

Recent reports from Bleeping Computer and Josh Lemon have highlighted the use of phishing attacks to deliver the DarkComet remote administration tool (RAT) as a malicious payload (e.g., (via PDF or zip file with an embedded malicious .scr). External web threats (e.g., malicious links, drive-by-downloads, watering holes, etc.) have also been leveraged to serve a typically obfuscated payload with pre-configured for server-client architecture.

Figure 1. Email with embedded .scr file that triggers DarkComet install - Source BleepingComputer



[redacted].com> [redacted]

Shipping docs#330

DOC000YUT600.pdf.z
1 MB

Dear sir,

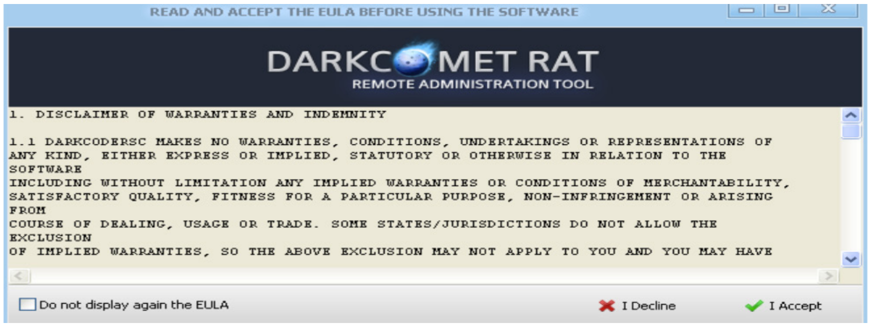
Please check the attached shipping docs for your confirmation, we have already sent the original documents to your bank to arrange the payment.

Thanks & Best Rgds
[redacted]
Landline-011-[redacted]
Mobile- :09[redacted], 09[redacted]

[redacted] Pvt Ltd
591, [redacted]
[redacted]
New Delhi-110038
Email: info@[redacted]
Website-[redacted]

The DarkComet RAT is an extremely versatile crimeware tool that provides robust capabilities for the efficient remote administration of compromised systems. A large number of different malicious campaigns and actors have utilized this RAT for years in order to facilitate identity theft, financial fraud, and more.

Figure 2. DarkComet RAT banner


READ AND ACCEPT THE EULA BEFORE USING THE SOFTWARE
DARKCOMET RAT
REMOTE ADMINISTRATION TOOL
□ Do not display again the EULA
I Decline
I Accept

```
1. DISCLAIMER OF WARRANTIES AND INDEMNITY

1.1 DARKCODERSC MAKES NO WARRANTIES, CONDITIONS, UNDERTAKINGS OR REPRESENTATIONS OF
ANY KIND, EITHER EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE IN RELATION TO THE
SOFTWARE
INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY,
SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OR ARISING
FROM
COURSE OF DEALING, USAGE OR TRADE. SOME STATES/JURISDICTIONS DO NOT ALLOW THE
EXCLUSION
OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU AND YOU MAY HAVE
```

Author
ROB SOTO
& KEVIN STEAR

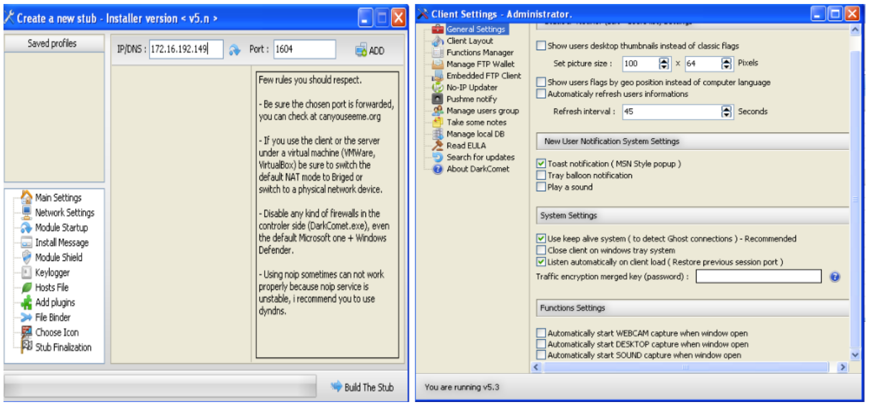
Jask Labs
TA-0015

TLP
WHITE

Risk Factor
MEDIUM

As an all-in-one administration tool, DarkComet provide actors with immediate access to functionality usually limited to multistage campaigns, and according to Kaspersky, the use of multifunctional (e.g., DarkComet) has increased considerably this year. (This uptick is believed to be related to improvements in network and endpoint defenses, which hinder actor success rates for the execution of multiple stage attacks and post-exploitation functions).

Figure 3. DarkComet RAT client/stub configuration



IP/DNS : 172.16.192.149 Port : 1604

Few rules you should respect.

- Be sure the chosen port is forwarded, you can check at canyouseeme.org

- If you use the client or the server under a virtual machine (VMWare, VirtualBox) be sure to switch the default NAT mode to Briged or switch to a physical network device.

- Disable any kind of firewalls in the controler side (DarkComet.exe), even the default Microsoft one + Windows Defender.

- Using noip sometimes can not work properly because noip service is unstable, i recommend you to use dyndns.

□ Show users desktop thumbnails instead of classic flags
Set picture size : 100 × 64 Pixels
□ Show users flags by geo position instead of computer language
□ Automaticaly refresh users informations
Refresh interval : 45 Seconds

New User Notification System Settings

☑ Toast notification (MSN Style popup)
□ Tray balloon notification
□ Play a sound

System Settings

☑ Use keep alive system (to detect Ghost connections) - Recommended
□ Close client on windows tray system
☑ Listen automatically on client load (Restore previous session port)
Traffic encryption merged key (password) :

Functions Settings

□ Automatically start WEBCAM capture when window open
□ Automatically start DESKTOP capture when window open
□ Automatically start SOUND capture when window open

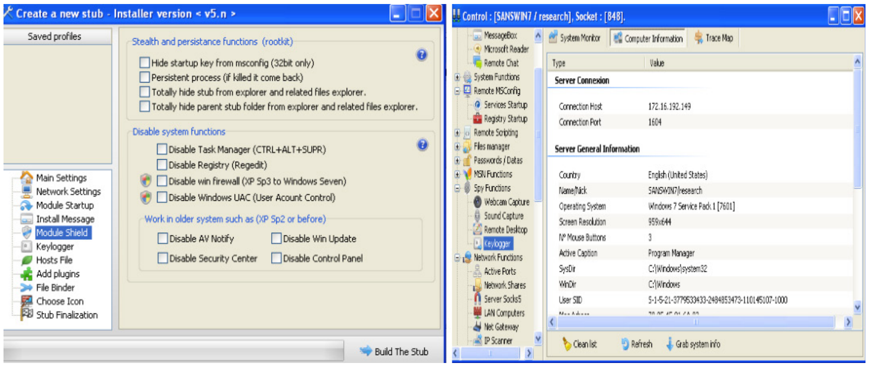
You are running v5.3

Multifunctional RATs like DarkComet can provide quick returns to malicious actors thanks to their ability to quickly deploy post-exploitation payloads and further entrenchment (DDoS, CryptoMining, Spam, etc). Also, since they are usually very simple to set up/build and deploy, these multifunctional tools require less effort and financial cost to run and maintain.

Lab/Field Study

The following screen-grabs were taken during proof of concept research of the DarkComet RAT and demonstrate the simplicity and effectiveness of multifunctional remote administration tools.

Figure 4. DarkComet RAT client entrenchment functions & victim system OS profile



Stealth and persistance functions (rootkit)

□ Hide startup key from msconfig (32bit only)
□ Persistent process (if killed it come back)
□ Totally hide stub from explorer and related files explorer.
□ Totally hide parent stub folder from explorer and related files explorer.

Disable system functions

□ Disable Task Manager (CTRL+ALT+SUPR)
□ Disable Registry (Regedit)
□ Disable win firewall (XP Sp3 to Windows Seven)
□ Disable Windows UAC (User Acount Control)

Work in older system such as (XP Sp2 or before)

□ Disable AV Notify □ Disable Win Update
□ Disable Security Center □ Disable Control Panel

Type	Value
Server Connexion	
Connection Host	172.16.192.149
Connection Port	1604
Server General Information	
Country	English (United States)
Name/Nick	SANSWIN7/research
Operating System	Windows 7 Service Pack 1 [7601]
Screen Resolution	959x644
N° Mouse Buttons	3
Active Caption	Program Manager
SysDir	C:\Windows\system32
WinDir	C:\Windows
User SID	S-1-5-21-3779533433-2484853473-110145107-1000

Author
ROB SOTO
& KEVIN STEAR

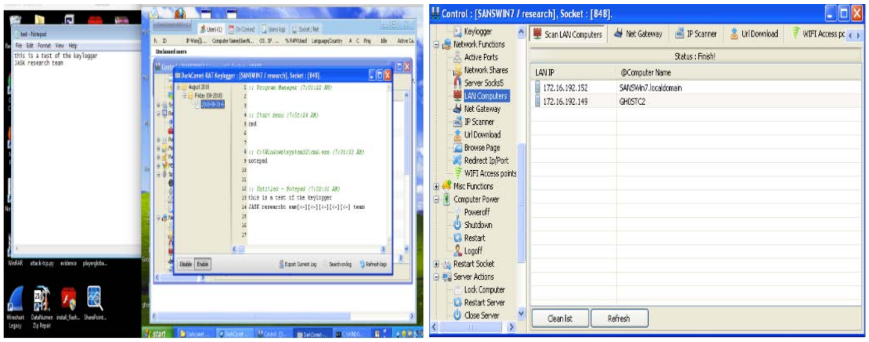
Jask Labs
TA-0015

TLP
WHITE

Risk Factor
MEDIUM

As seen above, DarkComet supports multiple entrenchment/evasion functions such as disabling Antivirus or User Account Control, which is typically a necessary step in order to escalate privileges and achieve persistence at a victim's system.

Figure 5. Two post exploitation functions such as Keylogger & LAN system discovery



```
this is a test of the keylogger
JASK research team
```

DarkComet-RAT Keylogger : [SANSWIN7 / research], Socket : [848].

```
1 :: Program Manager (7:01:22 AM)
2
3
4 :: Start menu (7:01:24 AM)
5 cmd
6
7
8 :: C:\Windows\system32\cmd.exe (7:01:32 AM)
9 notepad
10
11
12 :: Untitled - Notepad (7:02:32 AM)
13 this is a test of the keylogger
14 JASK research: sam[<-][<-][<-][<-][<-] team
15
16
17
```

Control : [SANSWIN7 / research], Socket : [848].

Status : Finish!

LAN IP	@Computer Name
172.16.192.152	SANSWin7.localdomain
172.16.192.149	GHOSTC2

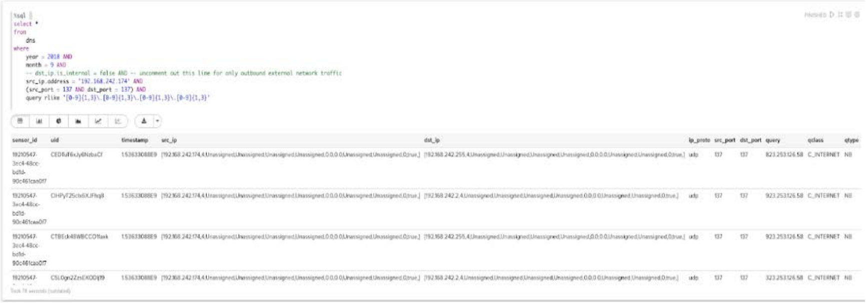
As seen in the above images, once installed on a victim's system, DarkComet can enable malicious actors to entrench and diversify post-exploitation crime monetizing tools -- a simple to use (yet very powerful) Swiss Army-knife-like crimeware weapon.

Detection

Because DarkComet has been an open-source capability for a number of years, it's behavior is relatively well understood. JASK's ASOC platform and can be relatively easily detect the RAT's presence in a host environment via network and log activity.

Like many other pieces of malware, the DarkComet RAT conducts a discovery phase during the setup process. One interesting aspect of this discovery is the use of externally bound NetBios queries for dot-decimal formatted data. Below are examples of using the ASOC's Zeppelin notebook to identify matching activity, and then craft corresponding Signal Logic.

Figure 6. ASOC Signal logic identifies DarkComet client side C2



```
%sql
select *
from
    dns
where
    year = 2018 AND
    month = 9 AND
    -- dst_ip.is_internal = false AND -- uncomment out this line for only outbound external network traffic
    src_ip.address = '192.168.242.174' AND
    (src_port = 137 AND dst_port = 137) AND
    query rlike '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}'
```

sensor_id	uid	timestamp	src_ip	dst_ip	ip_proto	src_port	dst_port	query	qclass	qtype
19210547-3ec4-48cc-bd1d-90c461caa0f7	CEDfuT6xJy6NzbaCf	1.53633088E9	[192.168.242.174,4,Unassigned,Unassigned,Unassigned,Unassigned,0.0.0.0,Unassigned,Unassigned,0,true,]	[192.168.242.255,4,Unassigned,Unassigned,Unassigned,Unassigned,0.0.0.0,Unassigned,Unassigned,0,true,]	udp	137	137	823.253.126.58	C_INTERNET	NB
19210547-3ec4-48cc-bd1d-90c461caa0f7	CIHPyT25ctx6XJFhq8	1.53633088E9	[192.168.242.174,4,Unassigned,Unassigned,Unassigned,Unassigned,0.0.0.0,Unassigned,Unassigned,0,true,]	[192.168.242.2,4,Unassigned,Unassigned,Unassigned,Unassigned,0.0.0.0,Unassigned,Unassigned,0,true,]	udp	137	137	923.253.126.58	C_INTERNET	NB
19210547-3ec4-48cc-bd1d-90c461caa0f7	CTBEck48WBCCO1axk	1.53633088E9	[192.168.242.174,4,Unassigned,Unassigned,Unassigned,Unassigned,0.0.0.0,Unassigned,Unassigned,0,true,]	[192.168.242.255,4,Unassigned,Unassigned,Unassigned,Unassigned,0.0.0.0,Unassigned,Unassigned,0,true,]	udp	137	137	923.253.126.58	C_INTERNET	NB
19210547-	CSLOgn2ZzsEXODij19	1.53633088E9	[192.168.242.174,4,Unassigned,Unassigned,Unassigned,Unassigned,0.0.0.0,Unassigned,Unassigned,0,true,]	[192.168.242.2,4,Unassigned,Unassigned,Unassigned,Unassigned,0.0.0.0,Unassigned,Unassigned,0,true,]	udp	137	137	323.253.126.58	C_INTERNET	NB

Took 18 seconds (outdated)

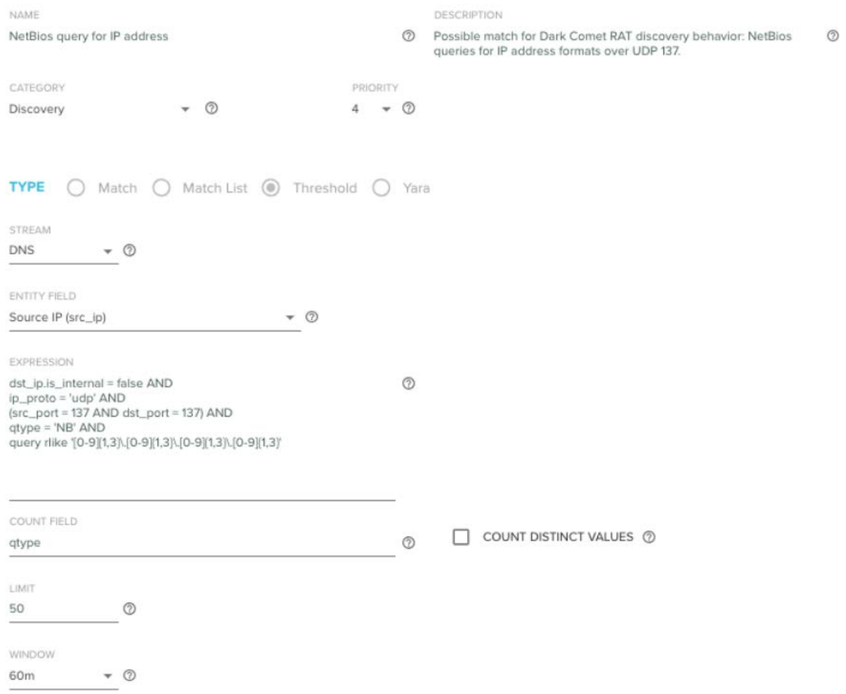
Author
ROB SOTO
& KEVIN STEAR

Jask Labs
TA-0015

TLP
WHITE

Risk Factor
MEDIUM

Figure 7. ASOC Signal logic identifies DarkComet client side C2



NAME
NetBios query for IP address

DESCRIPTION
Possible match for Dark Comet RAT discovery behavior: NetBios queries for IP address formats over UDP 137.

CATEGORY
Discovery

PRIORITY
4

TYPE ○ Match ○ Match List ● Threshold ○ Yara

STREAM
DNS

ENTITY FIELD
Source IP (src_ip)

EXPRESSION

```
dst_ip.is_internal = false AND
ip_proto = 'udp' AND
(src_port = 137 AND dst_port = 137) AND
qtype = 'NB' AND
query rlike '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}'
```

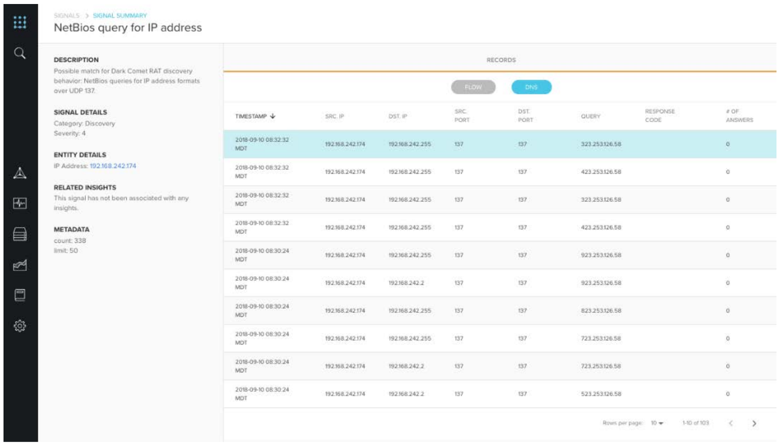
COUNT FIELD
qtype

□ COUNT DISTINCT VALUES

LIMIT
50

WINDOW
60m

Figure 8. ASOC Signal triggers on outbound NetBios queries for dot-decimal formatted data



NetBios query for IP address

DESCRIPTION
Possible match for Dark Comet RAT discovery behavior: NetBios queries for IP address formats over UDP 137.

SIGNAL DETAILS
Category: Discovery
Severity: 4

ENTITY DETAILS
IP Address: 192.168.242.174

RELATED INSIGHTS
This signal has not been associated with any insights.

METADATA
count: 338
limit: 50

TIMESTAMP ↓	SRC. IP	DST. IP	SRC. PORT	DST. PORT	QUERY	RESPONSE CODE	# OF ANSWERS
2018-09-10 08:32:32 MDT	192.168.242.174	192.168.242.255	137	137	323.253.126.58		0
2018-09-10 08:32:32 MDT	192.168.242.174	192.168.242.255	137	137	423.253.126.58		0
2018-09-10 08:32:32 MDT	192.168.242.174	192.168.242.255	137	137	323.253.126.58		0
2018-09-10 08:32:32 MDT	192.168.242.174	192.168.242.255	137	137	423.253.126.58		0
2018-09-10 08:30:24 MDT	192.168.242.174	192.168.242.255	137	137	923.253.126.58		0
2018-09-10 08:30:24 MDT	192.168.242.174	192.168.242.2	137	137	923.253.126.58		0
2018-09-10 08:30:24 MDT	192.168.242.174	192.168.242.255	137	137	823.253.126.58		0
2018-09-10 08:30:24 MDT	192.168.242.174	192.168.242.255	137	137	723.253.126.58		0
2018-09-10 08:30:24 MDT	192.168.242.174	192.168.242.2	137	137	723.253.126.58		0
2018-09-10 08:30:24 MDT	192.168.242.174	192.168.242.2	137	137	523.253.126.58		0

As another example, DarkComet passes client-server C2 (including it’s tell-tale banner ‘BF7CAB464EFB’) by default over TCP 1604, as shown below.

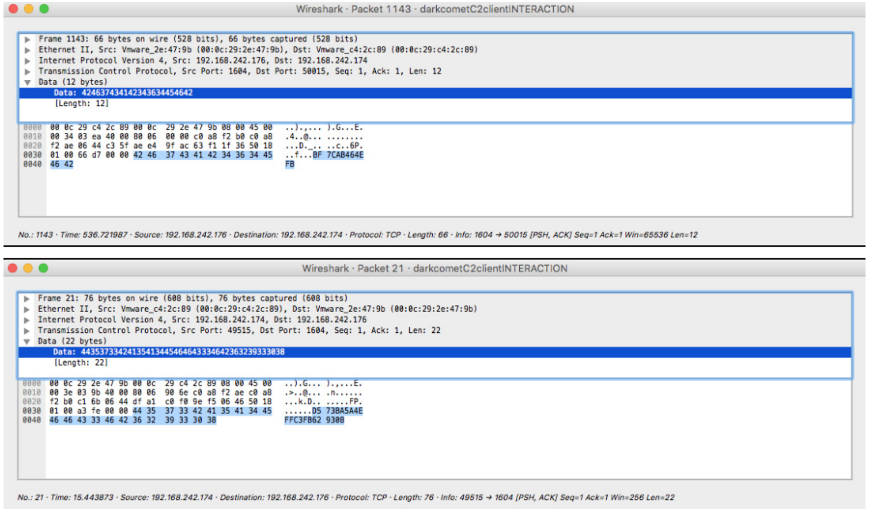
Author
ROB SOTO
& KEVIN STEAR

Jask Labs
TA-0015

TLP
WHITE

Risk Factor
MEDIUM

Figure 9. DarkComet C2 server-client interaction



```
▶ Frame 1143: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▶ Ethernet II, Src: Vmware_2e:47:9b (00:0c:29:2e:47:9b), Dst: Vmware_c4:2c:89 (00:0c:29:c4:2c:89)
▶ Internet Protocol Version 4, Src: 192.168.242.176, Dst: 192.168.242.174
▶ Transmission Control Protocol, Src Port: 1604, Dst Port: 50015, Seq: 1, Ack: 1, Len: 12
▼ Data (12 bytes)
    Data: 424637434142343634454642
    [Length: 12]

0000  00 0c 29 c4 2c 89 00 0c  29 2e 47 9b 08 00 45 00   ..).,... ).G...E.
0010  00 34 03 ea 40 00 80 06  00 00 c0 a8 f2 b0 c0 a8   .4..@... ........
0020  f2 ae 06 44 c3 5f ae e4  9f ac 63 f1 1f 36 50 18   ...D._.. ..c..6P.
0030  01 00 66 d7 00 00 42 46  37 43 41 42 34 36 34 45   ..f...BF 7CAB464E
0040  46 42                                              FB

No.: 1143 · Time: 536.721987 · Source: 192.168.242.176 · Destination: 192.168.242.174 · Protocol: TCP · Length: 66 · Info: 1604 → 50015 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=12
```

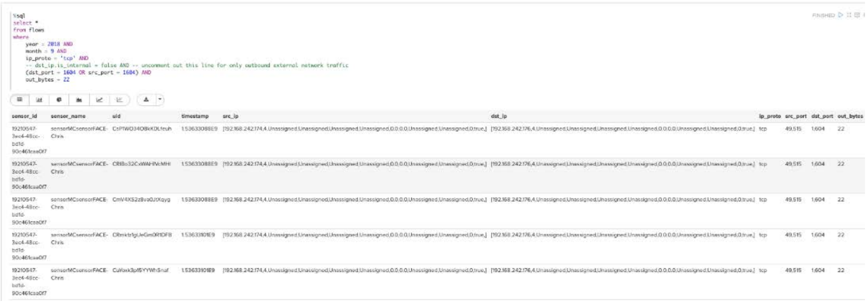
```
▶ Frame 21: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
▶ Ethernet II, Src: Vmware_c4:2c:89 (00:0c:29:c4:2c:89), Dst: Vmware_2e:47:9b (00:0c:29:2e:47:9b)
▶ Internet Protocol Version 4, Src: 192.168.242.174, Dst: 192.168.242.176
▶ Transmission Control Protocol, Src Port: 49515, Dst Port: 1604, Seq: 1, Ack: 1, Len: 22
▼ Data (22 bytes)
    Data: 44353733424135413445464643334642363239333038
    [Length: 22]

0000  00 0c 29 2e 47 9b 00 0c  29 c4 2c 89 08 00 45 00   ..).G... ).,...E.
0010  00 3e 03 9b 40 00 80 06  90 6e c0 a8 f2 ae c0 a8   .>..@... .n......
0020  f2 b0 c1 6b 06 44 df a1  c0 f0 9e f5 06 46 50 18   ...k.D.. .....FP.
0030  01 00 a3 fe 00 00 44 35  37 33 42 41 35 41 34 45   ......D5 73BA5A4E
0040  46 46 43 33 46 42 36 32  39 33 30 38               FFC3FB62 9308

No.: 21 · Time: 15.443873 · Source: 192.168.242.174 · Destination: 192.168.242.176 · Protocol: TCP · Length: 76 · Info: 49515 → 1604 [PSH, ACK] Seq=1 Ack=1 Win=256 Len=22
```

This activity is easily searchable via the ASOC's Zeppelin notebook (i.e. the Investigations tab). After which, users are able to field a custom Signal pattern within ASOC (specifically the content tab) to ensure that any future DarkComet activity will be automatically identified and contribute to the creation of potential Insights.

Figure 10. Zeppelin SQL logic identifies DarkComet client side C2



```
%sql
select *
from flows
where
    year = 2018 AND
    month = 9 AND
    ip_proto = 'tcp' AND
    -- dst_ip.is_internal = false AND -- uncomment out this line for only outbound external network traffic
    (dst_port = 1604 OR src_port = 1604) AND
    out_bytes = 22
```

sensor_id	senser_name	uid	timestamp	src_ip	dst_ip	ip_proto	src_port	dst_port	out_bytes
19210547-3ec4-48cc-bd1d-90c461caa0f7	sensorMCsensorFACE-Chris	CsPTWO34O8kKDLfeuh	1.53633088E9	[192.168.242.174,4,Unassigned,Unassigned,Unassigned,Unassigned,0.0.0.0,Unassigned,Unassigned,0,true,]	[192.168.242.176,4,Unassigned,Unassigned,Unassigned,Unassigned,0.0.0.0,Unassigned,Unassigned,0,true,]	tcp	49,515	1,604	22
19210547-3ec4-48cc-bd1d-90c461caa0f7	sensorMCsensorFACE-Chris	CRIBo32CxWAHPVcMHI	1.53633088E9	[192.168.242.174,4,Unassigned,Unassigned,Unassigned,Unassigned,0.0.0.0,Unassigned,Unassigned,0,true,]	[192.168.242.176,4,Unassigned,Unassigned,Unassigned,Unassigned,0.0.0.0,Unassigned,Unassigned,0,true,]	tcp	49,515	1,604	22
19210547-3ec4-48cc-bd1d-90c461caa0f7	sensorMCsensorFACE-Chris	CmV4XS2z8va0JtXqyg	1.53633088E9	[192.168.242.174,4,Unassigned,Unassigned,Unassigned,Unassigned,0.0.0.0,Unassigned,Unassigned,0,true,]	[192.168.242.176,4,Unassigned,Unassigned,Unassigned,Unassigned,0.0.0.0,Unassigned,Unassigned,0,true,]	tcp	49,515	1,604	22
19210547-3ec4-48cc-bd1d-90c461caa0f7	sensorMCsensorFACE-Chris	CRmktz1gUeGm0R1DF8	1.53633101E9	[192.168.242.174,4,Unassigned,Unassigned,Unassigned,Unassigned,0.0.0.0,Unassigned,Unassigned,0,true,]	[192.168.242.176,4,Unassigned,Unassigned,Unassigned,Unassigned,0.0.0.0,Unassigned,Unassigned,0,true,]	tcp	49,515	1,604	22
19210547-3ec4-48cc-bd1d-90c461caa0f7	sensorMCsensorFACE-Chris	CuYoxk3p15YYWhSnaf	1.53633101E9	[192.168.242.174,4,Unassigned,Unassigned,Unassigned,Unassigned,0.0.0.0,Unassigned,Unassigned,0,true,]	[192.168.242.176,4,Unassigned,Unassigned,Unassigned,Unassigned,0.0.0.0,Unassigned,Unassigned,0,true,]	tcp	49,515	1,604	22

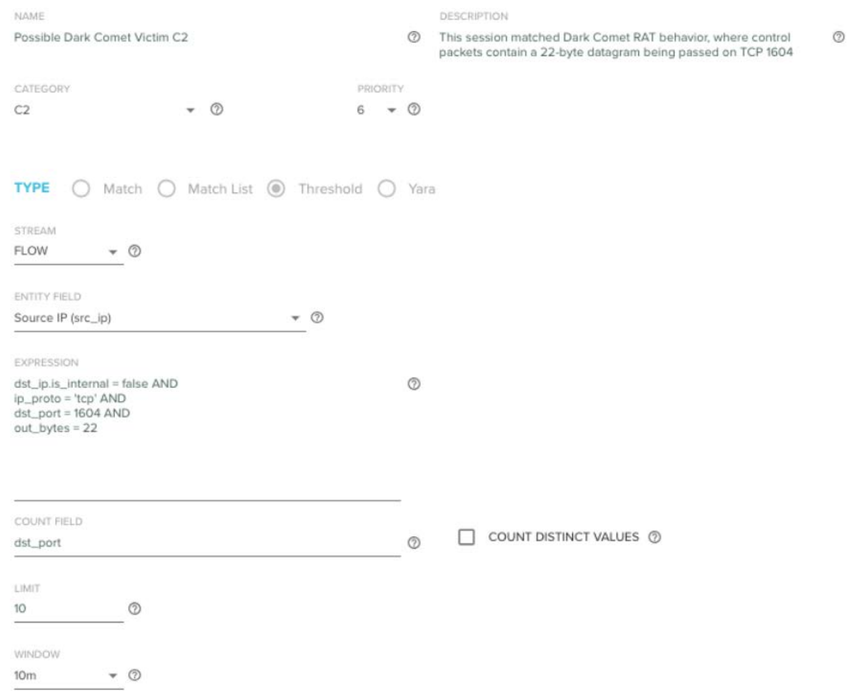
Author
ROB SOTO
& KEVIN STEAR

Jask Labs
TA-0015

TLP
WHITE

Risk Factor
MEDIUM

Figure 11. ASOC Signal logic identifies DarkComet client side C2



NAME
Possible Dark Comet Victim C2

DESCRIPTION
This session matched Dark Comet RAT behavior, where control packets contain a 22-byte datagram being passed on TCP 1604

CATEGORY
C2

PRIORITY
6

TYPE ○ Match ○ Match List ● Threshold ○ Yara

STREAM
FLOW

ENTITY FIELD
Source IP (src_ip)

EXPRESSION
```
dst_ip.is_internal = false AND
ip_proto = 'tcp' AND
dst_port = 1604 AND
out_bytes = 22
```

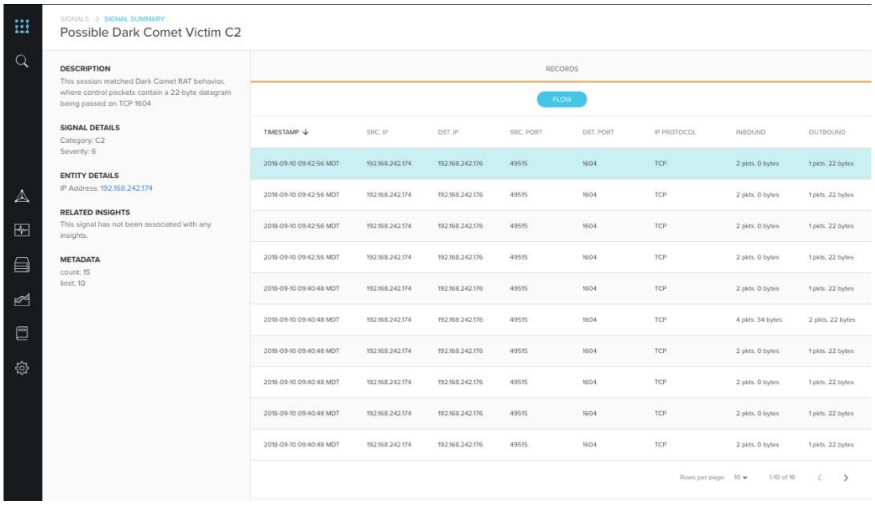
COUNT FIELD
dst_port

□ COUNT DISTINCT VALUES

LIMIT
10

WINDOW
10m

Figure 12. ASOC Signal triggers on DarkComet client side C2



SIGNALS > SIGNAL SUMMARY

Possible Dark Comet Victim C2

DESCRIPTION
This session matched Dark Comet RAT behavior, where control packets contain a 22-byte datagram being passed on TCP 1604

SIGNAL DETAILS
Category: C2
Severity: 6

ENTITY DETAILS
IP Address: 192.168.242.174

RELATED INSIGHTS
This signal has not been associated with any insights.

METADATA
count: 15
limit: 10

RECORDS

FLOW

TIMESTAMP ↓	SRC. IP	DST. IP	SRC. PORT	DST. PORT	IP PROTOCOL	INBOUND	OUTBOUND
2018-09-10 09:42:56 MDT	192.168.242.174	192.168.242.176	49515	1604	TCP	2 pkts, 0 bytes	1 pkts, 22 bytes
2018-09-10 09:42:56 MDT	192.168.242.174	192.168.242.176	49515	1604	TCP	2 pkts, 0 bytes	1 pkts, 22 bytes
2018-09-10 09:42:56 MDT	192.168.242.174	192.168.242.176	49515	1604	TCP	2 pkts, 0 bytes	1 pkts, 22 bytes
2018-09-10 09:42:56 MDT	192.168.242.174	192.168.242.176	49515	1604	TCP	2 pkts, 0 bytes	1 pkts, 22 bytes
2018-09-10 09:40:48 MDT	192.168.242.174	192.168.242.176	49515	1604	TCP	2 pkts, 0 bytes	1 pkts, 22 bytes
2018-09-10 09:40:48 MDT	192.168.242.174	192.168.242.176	49515	1604	TCP	4 pkts, 34 bytes	2 pkts, 22 bytes
2018-09-10 09:40:48 MDT	192.168.242.174	192.168.242.176	49515	1604	TCP	2 pkts, 0 bytes	1 pkts, 22 bytes
2018-09-10 09:40:48 MDT	192.168.242.174	192.168.242.176	49515	1604	TCP	2 pkts, 0 bytes	1 pkts, 22 bytes
2018-09-10 09:40:48 MDT	192.168.242.174	192.168.242.176	49515	1604	TCP	2 pkts, 0 bytes	1 pkts, 22 bytes
2018-09-10 09:40:48 MDT	192.168.242.174	192.168.242.176	49515	1604	TCP	2 pkts, 0 bytes	1 pkts, 22 bytes

Rows per page: 10 1-10 of 16

Author
ROB SOTO
& KEVIN STEAR

Jask Labs
TA-0015

TLP
WHITE

Risk Factor
MEDIUM

Mitigation

The best way to mitigate the threat of DarkComet infections is to prevent (or at a minimum detect) the delivery of the RAT. Some of the following items may prevent being infected by this threat.

- Do not open unsolicited or sketchy emails, especially from unknown sources
- Thoroughly check and scan any received attachment (or link), even if by trusted parties
- Avoid browsing unknown, high risk, pop-up websites
- Keep AV/NGAV and other security products patched and up to date
- Enforce minimum privilege at workstations/servers
- Create logic and monitor for possible DarkComet traffic

About JASK

JASK is modernizing security operations to reduce organizational risk and improve human efficiency. Through technology consolidation, enhanced AI and machine learning, the JASK Autonomous Security Operations Center (ASOC) platform automates the correlation and analysis of threat alerts, helping SOC analysts focus on high-priority threats, streamline investigations and deliver faster response times.

www.jask.com