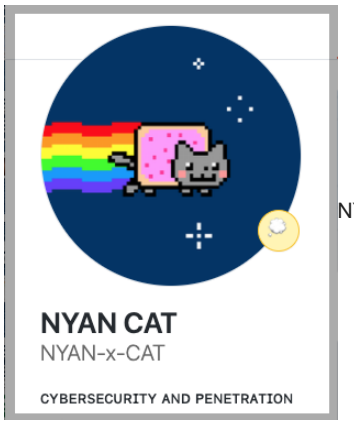
Possible Identity of a Kuwaiti Hacker NYANxCAT

redskyalliance.org/xindustry/possible-identity-of-a-kuwaiti-hacker-nyanxcat

October 19, 2020



NYANxCAT is a prolific hacker who programs new pieces and versions of malware, shares it widely, and records blackhat hacker educational YouTube videos which has over 150,000 views. He uses GitHub repository, sells his hacker tools and services using PayPal and Bitcoin. In this report, we discuss some of the samples of NYANXCat malware, his business models, and possible Kuwaiti identity.

(Figure 1. NYANxCAT GitHub logo)

NYANxCAT Hacker Profile

Name: possible name: Hmoud [Humooud] Meshal Aljraid [Al-Jerid].

Possible name in Arabic: حمود الجريّد.

Location: Likely location: Kuwait.

possible location: ST 58 HOUSE# 8, Jahra, Kuwait

Aliases: NYANxCAT, NYAN-x-CAT, NYAN_x_CAT, NYAN CAT, nyancat, NC, humooud.m, HumoudMJ, hmj_7, bomish3l.

Email: humooud.m@gmail.com, NYANxCAT@protonmail.com, NYANxCAT@pm.me

Profiles: github[.]com/NYAN-x-CAT “NYAN CAT”.

twitter[.]com/NYAN_x_CAT “n”, joined June 2016, posts starting July 2019.

twitter[.]com/HumoudMJ, joined December 2009.

Google ID: 106720573170316530671.

youtube[.]com/c/NYANCATx/about, started in Nov 20, 2018.

youtube[.]com/c/Bomish3l/, active 2013-2017.

pastebin[.]com/u/NYANxCAT PRO account started January 2018.

sellix[.]io/NYANxCAT.

Discord: NYANxCAT#0662 (Lime Server: 388 members).

Bitcoin: 12DaUTCemhDEzNw7cAFg9FndzcWkYZt6C8, 1jVe7d8GQB8z2ZqK6U8SCYAgeCJuYxaFo.

Hacker forums: hackforums[.]net, cracked[.]to.

Programming languages: C#, Visual Basic .NET, JavaScript

Programmed: LimeCrypter, VBS-Shell, Bitcoin Address Grabber v0.3.5, Lime-Miner, Lime-Dropper-1, Dropless-Malware v0.1, Csharp-Loader, Anti Analysis v0.2, Disable Windows Defender v1.1.

Edited/improved: Revenge-RAT v0.3, Neshta 1.0.

Languages: English, Arabic.

Details

NYANxCAT Possible Identity

NYANxCAT stays under the radar for Google/Youtube, PayPal, Github and other services, as he claims his blackhat hacking videos, tools, and malware are only “for educational purposes.” At the same time, NYANxCAT hides his real-life identity behind aliases. During his recent hacker career, he was also using semi-private tools such as Protonmail for communication and Bitcoin for donations and payments. Despite these measures, Red Sky Alliance analysts were able to analyze NYANxCAT’s communications and identify a possible hint to his real identity:

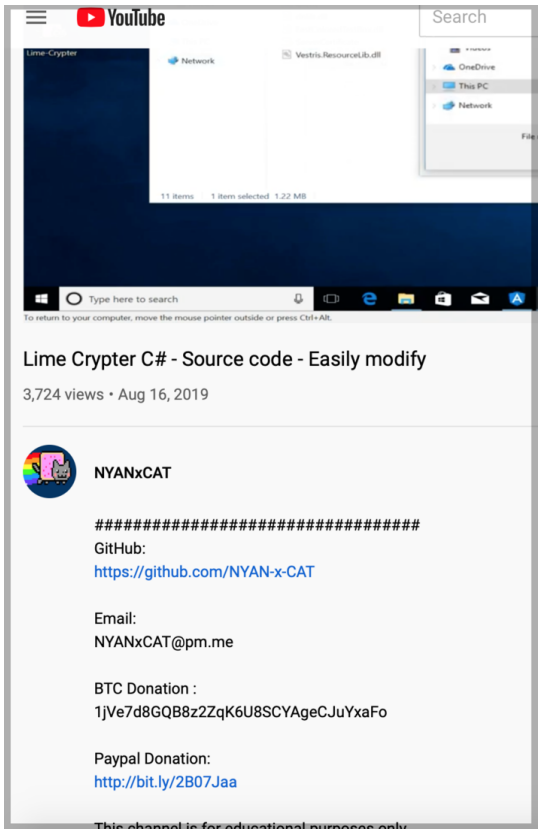


Figure 2. NYANxCAT hacking video and a PayPal donation link

Some of the NYANxCat’s hacking videos had a Paypal donation link given via an URL shortener: bit[.]ly/2B07Jaa (Figure 2).[1] This link is connected to Paypal hosted button id UEAXKSXDFJ2X6 and exposes email address humooud.m@gmail.com (Figure 3).

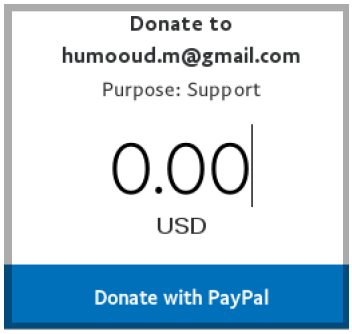


Figure 3. NYANxCAT linked PayPal page exposes his personal Gmail address

Analysis of the past uses of humooud.m@gmail.com shows that this email was used in 2017 to register domain odin-samsung[.]com. These records expose possible NYANxCAT identity as Hmoud Aljraid and his possible address in Jahra, Kuwait (Table 1).

Table 1. WHOIS historic record includes NYANxCAT’s email address

Domain Name:	odin-samsung[.]com

Time Period:	2017-02-09 – 2018-02-12
Registrant Name:	**Hmoud Aljraid**
Registrant Address:	ST 58 HOUSE# 8 Jahra KU 65852 KW
Registrant Phone:	965.9982545
Registrant Email:	**humooud.m@gmail.com**

Note that “Humooud” and “Hmoud” are likely the same Arabic name that could be written in English in more than two ways.

Additional research on humooud.m@gmail.com reveals that it is connected to Google User ID 106720573170316530671. That is listed as Humoud Meshal and is active leaving Google reviews in the vicinity of Kuwait City in the last 3 years, and Sri Lanka 6 years ago (Figure 4).[2]

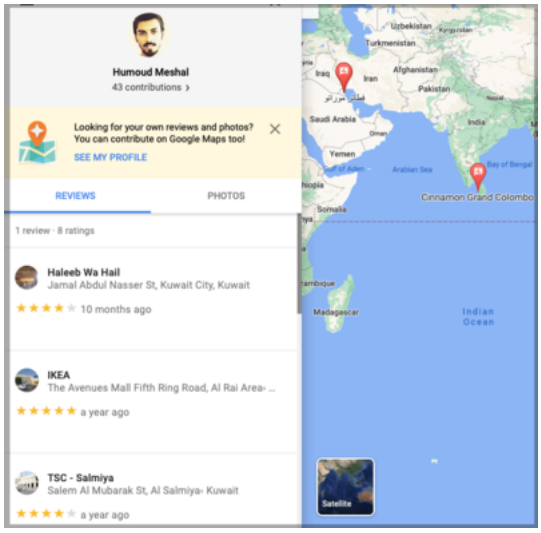


Figure 4. Humoud Meshal’s locations in Kuwait and Sri Lanka

Kuwaiti location matches cases when NYANxCAT actually put Kuwait as his country on his accounts (e.g. Github).[3] Past Sri Lankan location matches the nature of his past domain registration activity (Table 1). Most of NYANxCAT persona content is in English, but he is still able to have a conversation in Arabic as could be seen in some of his Youtube threads (Figure 5).

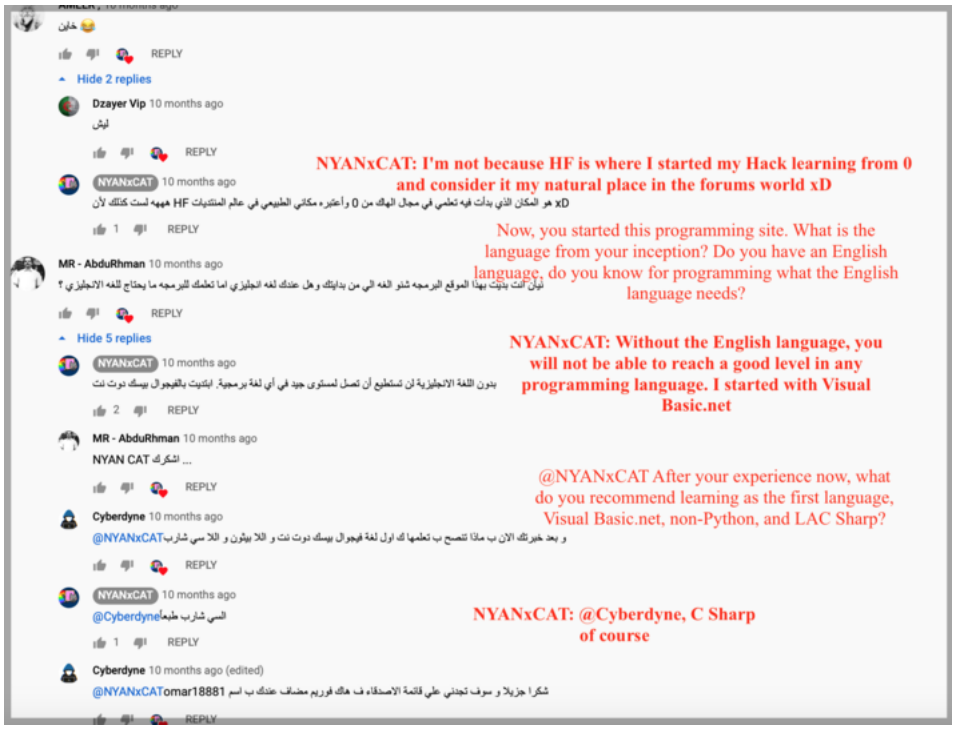


Figure 5. NYANxCAT is proficient in Arabic, Youtube comments

The search for Humoud Meshal's user picture reveals connection to technical Arabic blog bomish3l[.]com. This blog references additional Youtube "Bomish3l" and Twitter @HumoudMJ accounts (Figure 6).

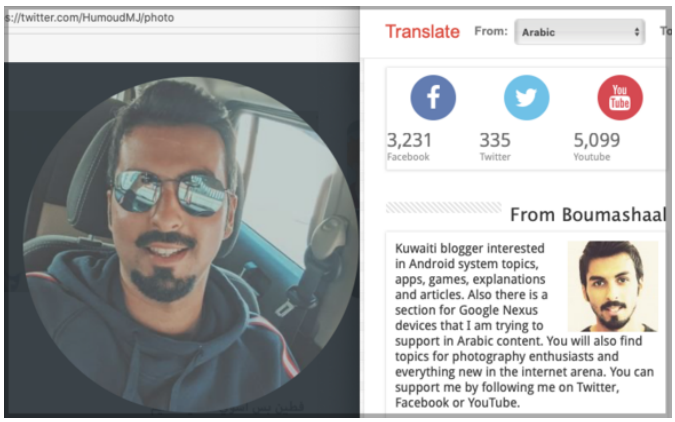


Figure 6. Humoud's photo on Twitter (left) and on his autotranslated blog (right)

Humoud's Twitter account, @HumoudMJ follows a number of exploit-related accounts. He lists his name in Arabic, that autotranslates as Hammoud Al-Jerid which matches the historic WHOIS record (Table 1).

Humoud's Youtube account had videos on a couple of topics including Android and hacking, e.g. video, "Hacking devices in wireless networks using your Android phone".[4] It is interesting that that YouTube account was posting videos since 2013, last one was in 2017. But in 2018, we see another YouTube channel becoming active: NYANxCAT.[5]

Humoud Meshal aka Humoud Aljraid uses aliases like HumoudMJ or hmj_7, so it is logical that Meshal is his middle name (M), while Aljraid/Al Jerid is his last [J].[6]

As NYAnxCAT and Humoud accounts are connected via the used PayPal and Gmail accounts, Kuwaiti location, hacking interest, and language capabilities, we assess with medium confidence that Humoud is the real NYANxCAT identity (see The NYANxCAT Hacker Profile above).

From Donations to Services

NYANxCAT was trying to monetize his notoriety in various ways. He would often include donation links into his source code and educational videos – often it was his Bitcoin addresses, sometimes PayPal donation link (see above, Figure 2,3).

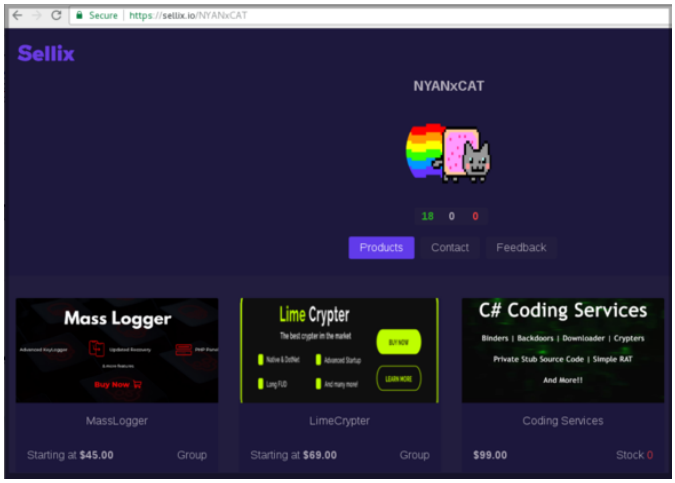


Figure 7. NYANxCAT hacker shop at Sellix as of July 2020

NYANxCAT created a personal shop page at Sellix. Earlier this year, he was selling three items: his C# hacking tools and malware coding services, his hacker tool Lime Crypter, and his malware Mass Logger (Figure 7). Later in October 2020, NYANxCAT removed the offer of the programming services, leaving the malware and the hacking tool for sale.

NYANxCAT Samples

We analyze various malicious samples associated with NYANxCAT – mostly recent ones from September 2020. These samples cover different stages of malicious attacks, some of them are source code and crypters used for weaponization – preparation of the attack. Some are the delivery mechanism for later stage malware. Others are installation artifacts. See the brief description below and the Indicators table attached. We also included some personal strings: emails, cryptocurrency addresses, aliases. Those are useful for the profile building, but they are also helping find new samples in the wild as they often have strings with NYANcCAT aliases or his Github page. When listing indicators, we do not include “NYAN CAT” alias as it brings some true positives, but also bring many false positive as it was an original popular meme name that was adopted by this hacker.

LimeCrypter

NYANxCAT programmed and is promoting and distributing his hacker tool called LimeCrypter (also Lime-Crypter). One of the latest LimeCrypter version seen in the wild is 2.0.7552.41963, executable sample hash:

f55a23559bb981f9a054297b003293b890b8caa2b7abccef9464b817787352a6.[7]

This hacker tool calls to NYANxCAT hidden paste on Pastebin for the list of recent upgrades and added features. It claims a first release date of 18 July 2020, and the last update as of this writing, 8 October 2020.[8] NyanxCAT Github shows that he was working on the LimeCrypter since at least August 2019, possibly since 2018.[9]

Figure 8. NYANxCAT’s Youtube video shows LimeCrypter made a malware undetectable

Since August 2020, NYANxCAT posted four videos explaining and promoting this hacker tool, showcasing how it helps to avoid antivirus detections (Figure 8).[10]

RATs

AsyncRAT by NYANxCAT can often be seen among samples in the wild. Executable sample hash:

22096a0846ab1399647bb2cc5596c649fa6508d2bd09db05476b27acd9d4eea2.[11] Async RAT can be detected using Yara rule win_asyncrat by Johannes Bader @viql.[12]

Archived sample containing another NYANxCAT-related RAT, Revenge-RAT v3, could be found using the following hash: 2cf26e5fe9f31386d57170cc51ec46d6e4b73e4760826d65ca1a7afc8c82acc2.[13]

Downloaders

A few small NYANxCAT related samples in the wild represent various downloaders (droppers). Those include JS Downloader, VBS Shell, and a number of unidentified droppers (see Indicators Table attached below). A sample of JS Downloader code with payload URL could be found using this hash:

5747ad762067a8a6617d2a4362304c24e11b21d6deed2da2adb31b8d55a4607c.[14]

Miners

Some of the NYANxCAT-related malware has cryptomining capabilities. One example is NYANxCAT-branded Lime Miner, executable sample hash:

74de28d70ee4bd414597561b696f865cb3c88fd3626161d36c423d35154e11a5.[15] Another example is a case of AsyncRAT.exe with Monero cryptocurrency mining capability (see Indicators below).

Modifications

It was also common for NYANxCAT to take an old piece of malicious code and to adapt/modify it for more malicious potential. Examples are Revenge-RAT v0.3, Neshta 1.0 – modified and branded by NYANxCAT.[16]

Waiving Responsibility

NYANxCAT often includes a waiver that his code is not for malicious use. But examining samples of code signed by NYANxCAT we can see them dropping ransomware, backdoors, and other kind of malware.[17] Moreover, studying NYANxCAT videos confirms those are not just sandbox exercises, but involve actual victims.

Conclusion

NYANxCAT started his blackhat hacker career in at least 2018. While he is not the most advanced, his opportunistic behavior and abuse of legitimate services such as YouTube and Github allows him to rapidly expand his criminal network and is negatively affecting the number of his victims.

Indicators

Indicator	Type	Kill_Chain_Phase	First_Seen	Last_Seen	Comm
9b62966982e91013c608f2542df01411704fe40c8d0cd63ced524f4ed33bab8d	SHA256	Weaponization	9/28/20	9/28/20	Lime versi 2.0.7
90c2bb06bf684b2e6204418abeee6c81a552d997b163599e8da60c035223a230	SHA256	Delivery	9/27/20	9/27/20	Drop
b7460d79341ad3ad3acd17703fbf9e1f3b1fdbd1cff7ab8e3607899ced8c61bc	SHA256	Installation	9/22/20	9/22/20	Asyn
5747ad762067a8a6617d2a4362304c24e11b21d6deed2da2adb31b8d55a4607c	SHA256	Delivery	9/25/20	9/25/20	JS D by N
github[.]com/NYAN-x-CAT	URL	Weaponization	10/13/17	10/14/20	Nyan malw repos
pastebin[.]com/raw/WJD0PWxV	URL	Weaponization	9/28/20	10/14/20	Lime calls for a log
humooud.m@gmail.com	Email	Weaponization	8/16/19	10/14/20	Nyan PayP emai

NYANxCAT@protonmail.com	Email	NA	10/15/19	10/14/20	Hack
NYANxCAT@pm.me	Email	NA	1/9/19	10/14/20	Hack
NYANxCAT	String	NA	1/9/19	10/14/20	Hack
NYAN_x_CAT	String	NA	1/9/19	10/14/20	Hack
NYAN-x-CAT	String	NA	1/9/19	10/14/20	Hack
12DaUTCemhDEzNw7cAFg9FndzcWkYZt6C8	String	Weaponization	5/27/19	10/14/20	Nyan Bitco
1jVe7d8GQB8z2ZqK6U8SCYAgeCJuYxaFo	String	Weaponization	1/9/19	10/14/20	Nyan Bitco
2cf26e5fe9f31386d57170cc51ec46d6e4b73e4760826d65ca1a7afc8c82acc2	SHA256	Weaponization	9/14/20	9/14/20	Reve v3 - NYAI
e62cc243c2bb10a2613a64f8b59ad27ec6f7592868902b6793dceb230b8f72bf	SHA256	Delivery	9/13/20	9/13/20	Drop
nyanxcat.vbs	File	Delivery	9/13/20	9/13/20	Drop
914b759c186e0cdb0e82c4bbbbd5257fd1c7a60db0e77bbc24778362ee549bce	SHA256	Delivery	9/13/20	9/13/20	Drop
f8890477e760cdb8f4a4fdbf8e8b5b1a224bc87046875b9ee17a9fcb93d2f118	SHA256	Exploitation	9/13/20	9/13/20	File t EXE
233587a133e3e112f42a5b456c94fca514d364f10b532291c1cc3c0aea92526e	SHA256	Delivery	9/11/20	9/11/20	Drop
ec5d16ff69ca2221bd60f41049f9862fe4cba0dd238959d78620140a00331250	SHA256	Delivery	9/11/20	9/11/20	Drop
54ea7614e8220bf4cad9ccd2c87d1470e341ef14b9d7c02ebe432a9c3139b8ab	SHA256	Installation	9/10/20	9/10/20	VBS-NYAI ASCI progr
http://f0439583.xsph[.]ru/Cryptolocker.exe	URL	Delivery	9/14/20	9/14/20	Rans
4b7bf7d3fac0ae3fe45a3d126bd07b65d5c824a5a423823f7c8900d9da4a1a1e	SHA256	Delivery	9/10/20	9/10/20	Drop
00714fae672b284458a4784ee651ed42bf51ec5fead0cf4c17082f75ac5f782b	SHA256	Weaponization	9/9/20	9/9/20	Bitco Grab
74de28d70ee4bd414597561b696f865cb3c88fd3626161d36c423d35154e11a5	SHA256	Installation	9/9/20	9/9/20	Lime 0.3.0 type EXE
f1ad4dbe66d9570c067889cbb0876c3771c6750e6e5a96c3d784336fcc5c88a4	SHA256	Weaponization	9/8/20	9/8/20	Lime 1.0.0
5882452922bf3c291f64ce3cfe5ad557dc8911a101495aa923fb3c521c0446fd	SHA256	Weaponization	9/8/20	9/8/20	Lime 1.0.0
aca10c4a756f850bbb748715d2b5ba1e3466a6309d630a99f834dcc61abfc945	SHA256	Weaponization	9/8/20	9/8/20	Lime 1.0.0

22096a0846ab1399647bb2cc5596c649fa6508d2bd09db05476b27acd9d4eea2	SHA256	Installation	9/7/20	9/7/20	Asyn
a74af46f97845d0da1d2e761b85f42664c77ca1f2378a3c1e22fc1d0e2dd5188	SHA256	Installation	9/7/20	9/7/20	VBS- NYAI ASCI progr
0430bad23899d3b9ec9e52f587e944075b793f55f3f2f32283910343668a6785	SHA256	Delivery	9/6/20	9/6/20	Drop
96de85fba7d85672bf59601c518aba429a8415089851772f66ae2df59848139b	SHA256	Delivery	9/4/20	9/4/20	Drop
2f7371a3095fceb9b99bcb2abc176a142c37ca95940c91c58d3321ed54310bd2	SHA256	Delivery	9/3/20	9/3/20	Drop
110716c7f7f1e2f7e4b6237015ee2855efac37b609977ad451c1b0c8b54d0b63	SHA256	Delivery	9/3/20	9/3/20	Drop
34f3f6477224c8e17c31fd434470ee098a621b2732b5e8d9ca59f2c6ef5acf57	SHA256	Installation	9/3/20	9/3/20	VBS- NYAI ASCI progr
9f5bfe12e454f8b67649e52cc064032f0b149492428729fdf7e8c41d6bec6fcb	SHA256	Installation	9/3/20	9/3/20	VBS- NYAI ASCI progr
https://pashupatipaints[.]com/test/minAZ34EXEitscr.exe	URL	Delivery	9/3/20	9/7/20	
f55a23559bb981f9a054297b003293b890b8caa2b7abccef9464b817787352a6	SHA256	Weaponization	9/24/20	9/24/20	Lime Versi 2.0.7
365ee8918af55945cfa1a4a8bf30b214814c23833261b3a67117a6237d961806	SHA256	Installation	9/23/20	9/23/20	
2e64a2918346eaa8b5441a6904d2741c37079456b00c91f2801a3d01c94f4dd5	SHA256	Installation	9/22/20	9/22/20	Drop
39f394baf297dcabc3bdcbc0f71b2f14a96d0e44df88a16d0f9e4f8bc2d3c3e6	SHA256	Installation	9/19/20	9/19/20	Drop
dced2da7db2861a40ac1a32cc5eb4d2205c0be6cf49f9f9bd2710fb98ee6cbc2	SHA256	Installation	9/18/20	9/18/20	Asyn
e7eb31d13152158739d663eeabf2dfde8455deb4a4ffa0587e45676583e5f7e7	SHA256	Installation	9/17/20	9/17/20	Nesh malw by N for p
8b226dc5916d9c78eb1e3790241128d2d4ce6cd0b9124230d7574e62f0a28f4c	SHA256	Weaponization	9/15/20	9/15/20	Lime Cryp versi
3e905ce85036d960c7f68c5fc7f848e1f9fb5c550d9e97998be111938b2ac0da	SHA256	Delivery	9/27/20	9/27/20	Drop
033859addb85933297132cf3dc356c2b3780f9e10638149ae9ec8559aae00930	SHA256	Delivery	9/3/20	9/3/20	Drop
4d4e12de934064e401442a81e83563bfb2c98fb845b115eb60e5b6ce3e2639e2	SHA256	Delivery	9/1/20	9/1/20	JS D
d64cb13bb5820b9618e5733537794b8de03a35387b626f26ce20921625dabf53	SHA256	Installation	8/31/20	9/26/20	Nesh malw by N for p

dbc0a745c62c9aef393f732f718149fc5abaffe30ddb1d55d978a8bf17e9ae01	SHA256	Weaponization	3/6/20	9/2/20	Reve v3 - NYAI
97ca0ed6e618f457b56df8201689affb1a4c5410d29e222730966a36b6176047	SHA256	Delivery	8/30/20	8/30/20	Lime Versi
6450208e47c71ac8bfb8dc35e3c37fbeb01c02c021b162352fc8eb44e03af3e6	SHA256	Delivery	8/28/20	8/28/20	Drop Shell CAT
431dea8a2af305cd0b8d735efbadb1a46f1025b96838bb8b282bab502b001f49	SHA256	Delivery	8/27/20	8/27/20	NJ R
165749a5f359e0316396cddd2e461f14f11756b62f786561019de99ded742af1	SHA256	Installation	8/26/20	8/26/20	Angr versi
eb8276581ad494331c5586593e9bd533e3545db82eeb00872e0685dc67546305	SHA256	Installation	8/25/20	8/25/20	Asyn with crypt minir

Download indicators in CSV format: IR-20-292-001_Hmoud Aljraid NYANxCAT.csv

Appendix A. Additional Imagery

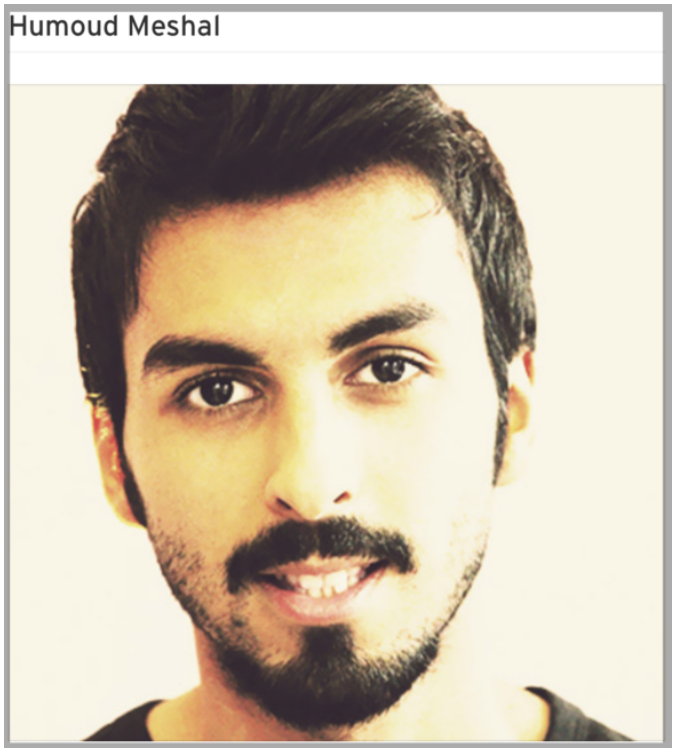


Figure 9. Humoud's Soundcloud Profile Picture

Serial: IR-20-292-001

Country: KW, US

Report Date: 20201018

Industries: All

Red Sky Alliance has been tracking hacker threats for the past 7 years. We are a Cyber Threat Analysis and Intelligence Service organization. For questions, comments, or assistance, please contact the lab directly at 1-844-492-7225, or feedback@wapacklabs.com.

Red Sky Alliance can help protect with attacks such as these. We provide both internal monitoring in tandem with RedXray notifications on ‘external’ threats to include, botnet activity, public data breaches, phishing, fraud, and general targeting.

https://www.wapacklabs.com/redxray

Red Sky Alliance is in New Boston, NH USA. We are a Cyber Threat Analysis and Intelligence Service organization. For questions, comments or assistance, please contact the lab directly at 1-844-492-7225, or feedback@wapacklabs.com

- Reporting: https://www.redskyalliance.org/
- Website: https://www.wapacklabs.com/
- LinkedIn: https://www.linkedin.com/company/64265941

[1] www.youtube[.]com/watch?v=N16d_zvIgTg

[2] google[.]com/maps/contrib/106720573170316530671/reviews/

[3] github[.]com/NYAN-x-CAT

[4] youtube[.]com/watch?v=30BV5U9OGv0, Jun 11, 2014.

[5] youtube[.]com/c/Bomish3l/videos

and youtube[.]com/c/NYANCATx/about

[6] soundcloud[.]com/hmj_7/

[7] virustotal[.]com/gui/file/f55a23559bb981f9a054297b003293b890b8caa2b7abccef9464b817787352a6/

[8] Pastebin[.]com/raw/WJD0PWxV

[9] github[.]com/NYAN-x-CAT/Lime-Crypter

[10] www[.]youtube[.]com/watch?v=_dYngLbXUno

[11] virustotal[.]com/gui/file/22096a0846ab1399647bb2cc5596c649fa6508d2bd09db05476b27acd9d4eea2/details

[12] virustotal[.]com/gui/file/504fc502fef2fceaae027edb0e037e4e39a0ee62ca9f15ab316c70e8d6e5b740/details

[13] virustotal[.]com/gui/file/2cf26e5fe9f31386d57170cc51ec46d6e4b73e4760826d65ca1a7afc8c82acc2/details

[14] virustotal[.]com/gui/file/5747ad762067a8a6617d2a4362304c24e11b21d6deed2da2adb31b8d55a4607c/content/strings

[15] virustotal[.]com/gui/file/74de28d70ee4bd414597561b696f865cb3c88fd3626161d36c423d35154e11a5/details

[16] virustotal[.]com/gui/file/e7eb31d13152158739d663eeabf2dfde8455deb4a4ffa0587e45676583e5f7e7/details

[17] 6450208e47c71ac8bfb8dc35e3c37fbeb01c02c021b162352fc8eb44e03af3e6

and virustotal[.]com/gui/url/922efd801fc095b488126248f7c55d3d897fc14376d4d22a48966427ee8a421a/detection

and 165749a5f359e0316396cddd2e461f14f11756b62f786561019de99ded742af1