

May 2023

# Cyber Threat Intelligence Summary



— assure —

*Welcome to our second monthly Threat Intelligence briefing. This month we're looking at a favoured adversary tactic, 'Living off the Land', the rise of Anonymous Sudan, 'Carpet Bombing' and a look at the threat actor dubbed APT-1. All this plus an update on the 3CX breach and Genesis Market takedown, which featured in last month's report.*

# Contents

<b>1</b>	<b>'LOL' – Living Off the Land</b>	<b>03</b>
<b>2</b>	<b>Anonymous 'Sudan'- or is it?</b>	<b>05</b>
<b>3</b>	<b>Carpet-Bombing - DDoS evolves</b>	<b>06</b>
<b>4</b>	<b>Update – 3CX breach &amp; Genesis Market takedown</b>	<b>07</b>
<b>5</b>	<b>APT-1</b>	<b>08</b>
<b>6</b>	<b>Summary</b>	<b>10</b>

## 'LOL' – Living Off the Land

Summer may be here, but we're not out foraging yet; with our cyber hats still firmly on, this kind of living off the land refers to an adversary making best use of their environment, post-breach.

A good EDR solution is going to alert on malicious tools, particularly off-the-shelf ones generated with platforms such as Metasploit or Cobalt Strike, hopefully they'd be caught even before execution as they made their way over the network and on to the compromised host. With the aim of becoming ever stealthier and avoiding these electronic tripwires before their mission is accomplished, attackers are increasingly looking to leverage legitimate applications and utilities that are native to your operating system or application set. The distinct adversarial advantage here is that these are signed binaries, libraries or drivers often forming part of the operating system itself and in some cases, critical to its operation. Executables such as PowerShell, WMIC & MSBuild.exe are part of the modern Microsoft Windows OS and carry a valid digital signature from the vendor, as well as having powerful capabilities and running with System privileges. By taking this approach, an attacker is able to access stored credentials, bypass security measures such as UAC, move laterally across the network and ultimately, exfiltrate your data.

If your adversary is able to accomplish their mission using this technique alone, there will be no trace of malicious artefacts and when using a compromised account, the execution of legitimate applications may only serve to muddy the waters of an investigation.



For administrative reasons these legitimate tools are likely to be on your organisation's allow list, making them harder to restrict and harder still to detect when being used maliciously.

When fully considered, the above is starting to sound like the stuff of network defenders' nightmares! Thankfully, there are still defensive techniques we can deploy and online resources that we can use to detect this behaviour. The folks at the [LOLBAS Project](#) do an excellent job of curating the many Windows binaries that are susceptible to abuse as well as helpfully mapping them to the corresponding [MITRE ATT&CK](#) framework tactics. Their sibling site [LOLDrivers](#) does an equally comprehensive job of listing vulnerable Windows drivers, with a matured user interface and a wealth of related information, while [GTFOBins](#) presents the Unix-based OS equivalents of the LOLBAS project.

Being armed with these resources certainly helps, but what can you do when it comes to positive, defensive action? Know your network and know what's 'normal' – the basis of **anomaly detection** is to properly understand your activities using **behavioural analysis** and using that data to create intelligent tuning rules that recognise this activity. Anything outside of that behaviour, for example a non-technical user running powershell.exe to invoke the certificate signing tool, should still light up your SIEM like Blackpool seafront. Another critical function is **Threat Hunting** – deploying your human resource to look for signs of malicious activity using endpoint and network forensic techniques, correlating against known IOCs in order to prove or disprove their hypothesis. This is a skill that should never be underestimated, there are as many cases of criminal activity being uncovered by a tenacious analyst as there are from an IDS or EDR solution.



Finally, understand what coverage you have from your current Microsoft licences and ensure this meets with your expectations (get in touch if you need help with this) - check to see if you have 'Defender for Endpoint Plan 2' included and if not, consider upgrading to it. This security product from the vendor integrates natively with your Windows 10/11 desktop operating systems and provides EDR, discovery, threat analytics and advanced hunting functions and has a seamless integration with e2e-assure's bespoke SIEM, Cumulo. This allows our Analyst teams to see alert data from across your estate in real-time and respond accordingly. If you'd like to learn more about this service, or just want to talk LOLBins, get in touch!



## Anonymous 'Sudan'- or is it?

Over the last few weeks, we've seen increasing amounts of activity from a group calling itself 'Anonymous Sudan'. They are not a new organisation, having been around since at least 2019 in their original incarnation and are well-known for their use of DoS attacks, website defacements and general cyber vandalism, broadly in the name of pro-Sudanese interests and resisting attempts at government censorship. While last month's attacks on the Israeli Supreme Court and the Israel Post website still indicate a stance in the Arab world, 'Anonymous Sudan 2.0' as we're referring to them appear to have shifted focus considerably to be much more aligned with Russian interests, even declaring themselves to now be a part of [Killnet](#).

Their targeting appears to have followed the same, fundamental shift too – from only targeting organisations or countries whose actions were negatively impactful on their namesake country, '2.0' now appear to be engaging in a free-for-all across the Western hemisphere, attacking those with little or no connection to Sudan, but with plenty to Russia or in relation to the ongoing Ukraine conflict. Most recently, Sweden has come under sustained fire allegedly for the actions of [Rasmus Paludan](#) in burning a copy of the Quran but more likely for Sweden's signalled intent to join NATO, along with Russia's other neighbour, Finland.

Multiple TTPs have altered; the majority of 'Anon' operations favour Twitter as the social media platform for choice whereas Russia-aligned threat actors appear to favour Telegram, which is also the chosen platform for 'Anonymous Sudan 2.0' whose Telegram

channel is listed as being located in Russia and where the majority of posts are new appearing in Russian & English and not Arabic. Their post links also favour Killnet & Anonymous Russia and appear to have little interaction with other 'Anon' groups in the Arab world.

e2e-assure have been following both threat groups for some time and while we are keeping an open mind, we are now tracking these entities as individual threat actors and lean towards the hypothesis that the newer group is actually a Russian threat actor masquerading as Anonymous Sudan. Aside from the attack on Scandinavian Airlines (for which the Ransom payment exploded from \$3,500 to £175,000 in a matter of hours), 2.0 have also attacked Tinder in the last week, taken pot shots at both sides of the political divide in the Middle East and are reportedly lining up to strike at assets connected with Elon Musk, allegedly to 'encourage' him to make Starlink available in Sudan. We have to wonder, is it the lack of the technology in Sudan or its notable presence in Ukraine, particularly given its apparent [infrastructure support](#) for Ukrainian drone attacks.



There is a final twist to this speculation – according to [this report](#), the Wagner group have long been active across the African continent and nowhere more so than Sudan

“

Sudan has long been a particular focus for Wagner mercenaries, and there are many of them there. Back during the rule of the dictator Omar al-Bashir, who was in power from 1993 to 2019, licences already went to the Russian firm "M-Invest," which is probably under the control of oligarchs, including Wagner boss Yevgeny Prigozhin. This led to Wagner members being given the job of protecting the M-Invest gold mines in Sudan.

”



## Carpet-Bombing - DDoS evolves

Distributed, Denial of Service attacks are not new, but until recently the '(D)istributed' has referred to the attack emanating from multiple source locations, overwhelming the victim with parallel floods of traffic and from more than one location. Carpet-Bombing, also known as spread-spectrum or 'spray' attacks follow the same principle, but instead aims the attack at multiple IP addresses associated with the victim, in some cases across large swathes of publicly routable address space.

According to a recent DDoS CTI report shared by one of our contemporaries, 2022 saw a 300% increase in these types of attacks

over the previous year within the IPv4 space and 600% in IPv6, with an increased tendency to factor in reflection, flooding and packet fragmentation techniques. To give an idea of the scale of data involved in this practice, anything under 25Gbps (Gigabits per second) is classified as 'small' with the average appearing to be around 4.9Gbps in 2022, whereas the highest boasted a bandwidth consumption of a mammoth 1.3Tbps (Terabits per second), which is enough to make even the 'big three' sit up and take notice!

Traditionally, upstream service providers have

managed DDoS attacks by sink-holing (null routing) attack traffic off the network, which while protecting the wider network from saturation, ironically completes the denial of service attack by removing all traffic destined for the intended victim. Because carpet-bombing by its nature is less discriminatory, the attack is likely to cause massive collateral damage and make it extremely hard if not impossible to identify the true target. It is not unfeasible to consider that such an attack may impact an entire datacentre when the targeted IP space is contained entirely within their networks.

In order for your DDoS mitigation solution to remain effective, it should have the ability to analyse your Internet presence holistically and report on activity in such a way as to be insightful to the defenders. It should also scale with you and have the ability to incorporate additional infrastructures without necessitating a re-write or redeployment of sensors. Consider a managed service solution to complement your IRP with experienced professionals who are familiar with mitigating these types of attack.

source: <https://go.corero.com/threat>

## Update – 3CX breach & Genesis Market takedown

*Last month we reported on the supply-chain attack against VoIP solutions provider 3CX and also the law enforcement multi-agency takedown operation against the dark web marketplace 'Genesis'. Now that the dust has settled, we take a look at the developments since our original coverage.*

### 3CX breach

We reported in April that 3CX had fallen victim to a double supply-chain attack, being breached in turn following the previous compromise of the X\_Trader software which happened to be installed on a corporate endpoint, from where the attacker was able to pivot inside 3CX's own development infrastructure. Following investigations, it has now been confirmed that this was the work of North Korean-attributed threat actor LAZARUS, according to [Kaspersky](#) who also found that a backdoor named GOPURAM infected devices of some 3CX customers as a second-stage payload.

The whole incident appears to have been a wake-up call for 3CX who have strongly focused on security measures in the application development lifecycle and in their overall security posture as highlighted

in multiple blog posts from CEO Nick Galea through their [official site](#). We continue to monitor and have developed custom rule sets to detect & observe any related activity.



Image: BBC

## Genesis Market takedown

Despite a multi-agency takedown effort from law enforcement across the world, the Genesis Market was back up within a matter of days. Principal security research Cyril Noel-Tagoe was quoted in [SC Magazine](#) as saying

“

The roots of Genesis Market's operation, namely the administrators, darknet website, and malicious software infrastructure, have survived

”

Officials in the USA have speculated that the server infrastructure is operated from Russia, meaning that any hope of co-operation from their counterparts there is optimistic at best. While the barrier for entry has been raised marginally by the fact that the surface web version of the site remains offline, the dark web version remains active and trading. Until such a time as there is a truly international and co-ordinated response to cyber crime (a utopian ideal!) then we envisage this electronic version of whack-a-mole to continue indefinitely.

## APT-1

For almost twenty years, APT-1 have been regarded as one of the most prolific and active threat activity groups associated with China. Not just China, but as its Military Unit Designator indicates, Unit-61398 of the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, at the core of the Chinese military. Also known as 'Comment Crew', 'Comment Panda' and 'GIF89a' among other associated names, the epitomise the 'APT' moniker – they are Advanced, Persistent and very much a Threat.

Their main attack focus appears to be on the USA, however attacks have been attributed to them across the world, including the UK, Europe, Japan, Taiwan and South Africa and in multiple industries from high-tech to agriculture.

The primary motivator appears to be data theft, leveraged through the use of targeted phishing campaigns, hijacked FQDNs and a sprawling C2 infrastructure. The excellent MITRE ATT&CK resource has a [page](#) dedicated to their technical history, including TTPs and malware families which can be used as a starting point for rule and use case development and for further reading.

In 2021, global cyber security firm Mandiant undertook a comprehensive and incredibly detailed deep-dive into APT-1 which can be found [here](#). To supplement this report, they also released a complementary video on YouTube using real-world examples. They also released a complementary [video](#) on YouTube using real-world examples.



# How does **e2e-assure** protect you against APT-1 and other threat actors?



By collating and analysing high-quality IOCs, we ensure we remain in the most updated position of situational awareness; identifying new tactics, malicious infrastructure and attack trends as soon as they emerge.



Undertaking red-teaming and adversary emulation engagements ensures our teams are well-versed in adversary TTPS, meaning that these will be quickly recognised in a real-world scenario.



By informing and educating our clients through regular and exceptional threat briefs and publications such as this, we aim to share and disseminate actionable intelligence in order to encourage defensive security postures and raise awareness of emerging threats and campaigns.

What can you do to help yourself? As with our previous highlight of APT-43 (e2e-assure CTI briefing April 2023), our baseline advice remains the same – **Educate** your staff to spot malicious activity, **Patch** all systems regularly but especially those that are exposed to the public Internet and **Detect**

incoming attacks using a mature, defensive approach such as the one offered by e2e-assure. Together, we can be stronger.



## Let's connect!

Thanks for taking the time to read our briefing, we're happy to provide further information on any of the topics we've covered here.

We love having conversations about and helping people with Cyber Threat Intelligence, drop us an email - [cti@e2e-assure.com](mailto:cti@e2e-assure.com)