

Who are the latest targets of cyber group Lyceum?

prevailion.com/latest-targets-of-cyber-group-lyceum/

November 10, 2021



PREVAILION + **accenture**

9 November 2021

By Accenture Cyber Threat Intelligence and Prevailion Adversarial Counterintelligence Team

Prevailion's Adversarial Counterintelligence Team and Accenture's Cyber Defense group are teaming up to jointly utilize their respective proprietary data and expert analysis to deliver timely and in-depth security research. Our goal is to provide insights into threat actor tactics, targets, and campaigns to deliver actionable detection and mitigation opportunities to defenders.

Accenture's Cyber Threat Intelligence (ACTI) group and Prevailion's Adversarial Counterintelligence Team (PACT) dug into recently publicized campaigns of the cyber espionage threat group Lyceum (aka HEXANE, Spirlin) to further analyze the operational infrastructure and victimology of this actor. The team's findings corroborate and reinforce previous [ClearSky](#) and [Kaspersky](#) research indicating a primary focus on computer network intrusion events aimed at telecommunications providers in the Middle East. Additionally, the research expands on this victim set by identifying additional targets within internet service providers (ISPs) and government agencies. Although all victim-identifying information has been redacted, this report seeks to provide these targeted industry and geographic verticals with additional knowledge of the threat and mitigation opportunities.

Findings:

The ACTI/PACT team made the following key findings:

- Between July and October 2021, Lyceum backdoors appear to have targeted ISPs and telecommunication operators in Israel, Morocco, Tunisia, and Saudi Arabia as well as a ministry of foreign affairs (MFA) in Africa.
- At least two of the identified compromises are assessed to be ongoing despite prior public disclosure of indicators of compromise (IOCs).
- Domain name system (DNS) tunneling appears to be used only during the early stages of backdoor deployment; subsequently, the Lyceum operators use the HTTP(S) command and control (C2) functionality encoded in the backdoors.

Methodology:

From an offset in the comprehensive analysis by [ClearSky](#) and [Kaspersky](#), ACTI and PACT have conducted research on these campaigns based on Prevailion's network telemetry overlaid with ACTI's technical understanding of Lyceum backdoor communication.

The joint ACTI/PACT research team was able to identify additional web-based infrastructure used by Lyceum, which corroborated previous reporting and identified six domains with a previously unknown connection to Lyceum (five of which are currently registered). This research eventually fueled Prevailion's ability to annex over 20 Lyceum domains, which provided network telemetry of ongoing compromises. Analysis of this telemetry, enriched and corroborated with host-based data, allowed the team to identify additional victims and provide further visibility into Lyceum's targeting methodology.

Victimology:

Active since 2017, Lyceum targets organizations in sectors of strategic national importance, including oil and gas organizations and telecommunications providers. ACTI/PACT assess the targets for this campaign to be congruent with Lyceum's previous activity, however, the group has expanded its target set to include ISPs and government bodies.

ACTI/PACT identified victims within telecommunication companies and ISPs in Israel, Morocco, Tunisia, and Saudi Arabia as well as an MFA in Africa. Telecommunications companies and ISPs are high-level targets for cyber espionage threat actors because once compromised, they provide access to various organizations and subscribers in addition to internal systems that can be used to leverage malicious behavior even further. Additionally, companies within these industries can also be used by threat actors or their sponsors to surveil individuals of interest. MFAs are also highly sought-after targets because they have valuable intelligence on the current state of bilateral relationship and insight into future dealings.

Investigation Summary:

During this campaign, Lyceum used two primary malware families, dubbed Shark and Milan (a.k.a. James). The ACTI/PACT investigation focused on the C2 communication aspects that analysts observed in Prevaillon's telemetry, since [ClearSky](#) and [Kaspersky](#) have already provided detailed technical descriptions of the backdoors. Both backdoors can communicate via DNS and HTTP(S) for C2 communication (see Detailed Technical Description below for more information).

Shark produces a configuration file that contains at least one C2 domain, which is used with a Domain Generating Algorithm (DGA) for DNS tunneling or HTTP C2 communications. The C2 domains' authoritative name server is attacker controlled allowing Lyceum operators to provide commands through IP-addresses in the A-records of DNS responses. Shark uses a specific syntax when sending HTTP requests that enabled ACTI/PACT researchers to create a regular expression – a combination of characters in strings that specify a search pattern – to identify additional victims of the campaign. Using this regular expression, the researchers were able to pivot from likely Israeli hosts to IP-addresses resolving to telecommunication and ISPs in Israel and Saudi-Arabia. The backdoor had consistent beaconing at these victims beginning in September through October 2021.

For C2 communications over DNS, Milan uses hardcoded domains as the input for a custom DGA. The DGA is documented in [Kaspersky's](#) report as is some of the syntax used by Milan for C2 over HTTP(S). However, ACTI found that some of the legacy Milan backdoors retrieve data by generating requests using the hard-coded domain and then requesting one of a number Active Server Pages-related URL paths. These URL paths are hardcoded within some of the Milan samples. Those identified by ACTI were:

- contact.aspx
- default.aspx

- [preview.aspx](#)
- [team.aspx](#)

When the ACTI/PACT team queried the Prevailion dataset for the above-referenced, known, hard-coded URL paths observed in Milan samples, the team observed continued beaconing in October from an IP address that resolved to a telecommunications operator in Morocco.

Following this investigation thread, the ACTI/PACT team identified beaconing from a reconfigured or possibly a new Lyceum backdoor in late October 2021. The observed beacons were seen egressing from a telecommunications company in Tunisia as well as an MFA in Africa. The URL syntax of the newly reconfigured backdoor is similar to those generated in the newer version of Milan, however because the URL syntax is configurable, it is likely that the Lyceum operators reconfigured the URL syntax used by Milan to circumvent intrusion detection systems (IDS) and intrusion prevention systems (IPS) that were encoded to detect the previous Milan beacon syntax.

Outlook:

ACTI/PACT assess that Lyceum is likely updating its backdoors in light of recent public research into its activities to try and stay ahead of defensive systems. The group has continued its targeting of companies of national strategic importance. Lyceum will likely continue to use the Shark and Milan backdoors, albeit with some modifications, as the group has likely been able to maintain footholds in victims' networks despite public disclosure of IOCs associated with its operations.

To learn more about this threat actor and obtain additional behavioral analytics and detection opportunities, please contact info@prevailion.com

Mitigation:

Accenture and Prevailion provide the following detection opportunities and IOCs to aid enterprises within the targeted industries and verticals in detecting Lyceum activity.

Detection Opportunities for Shark:

Shark uses randomly generated directories to stage files for upload or after download. Below is an example:

```
c:\users\lukesdesktop\winlangdbdir468526d1102461
```

(See also Image 1 in the Detailed Technical Description)

The directories always appear to be appended by the filename of the Shark payload (e.g., winlangdbdir) and end with a 14-digit alphanumeric string (e.g., 468526d1102461). Detection engineers or network defenders are encouraged to look for similar directories on clients and servers in their networks.

Shark HTTP telemetry will match the following URL syntax:

```
///?q=\[a-z0-9\]{8}\(-\[a-z0-9\]{4}\){3}-\[a-z0-9\]{12}&qi=\[A-Za-z0-9%\]{16}&q1=
```

The URL syntax used by the new or reconfigured Lyceum backdoor is matched by the following regular expression:

```
///?\(proto|kind|pt\)=\[0-9\]{1}&\(index|pi|serv\)=
```

Detection Opportunities for Milan:

Defenders can use the following YARA rule to sweep their filesystems for the presence of Milan:

```
rule Milan
{
  meta:
    author = "ACTI"
    date = "2021-06-03"
    description = "matches ping, PDB strings and User-Agent syntax from the MilanRAT backdoor"
    hash = "b46949feeda8726c0fb86d3cd32d3f3f53f6d2e6e3fcd6f893a76b8b2632b249"
    hash1 = "d3606e2e36db0a0cb1b8168423188ee66332cae24fe59d63f93f5f53ab7c3029"
    hash2 = "21ab4357262993a042c28c1cdb52b2dab7195a6c30fa8be723631604dd330b29"
    hash3 = "a2754d7995426b58317e437f8ed6770cd7bb7b18d971e23b2b300b75e34fa086"
    hash4 = "b766522dd4189fef7775d663e5649ba9d8be8e03022039d20848fcbc3643e5f2"
    hash5 = "b54a67062bdcd32dfa9f3d7b69780d2e6e4925777290bc34e8f979a1b4b72ea2"
    strings:
      $re = /cmd.exe /C ping ([0-9]{1}.{1}){3}[0-9]{1} -n [0-9]{1}/ wide
      $a1 = "Mozilla/5.0" wide
      $a2 = "rmdir" wide
      $b2 = "C:\Users\kernel\Desktop\milan\Release\Milan.pdb" ascii wide
      $b3 = "Milan-asdsad-asd23-23-ad234-213-sad" ascii wide
      $b4 = "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.0.3705; .NET CLR 1.1.4322; Media Center PC 4.0; .NET CLR 2.0.50727)" ascii wide
      $b5 = "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36" ascii wide
    condition: uint16(0) == 0x5A4D and filesize > 800KB and $re and (all of ($a*) or 2 of ($b*))
}
```

Indicators of Compromise:

Defenders should query their network logs for any traffic matching the following Lyceum C2 domains:

- defenderlive[.]com
- dnsstatus[.]org
- wsuslink[.]com
- akastatus[.]com
- updatecdn[.]net
- dnscdn[.]org
- sysadminnews[.]info

- windowsupdatecdn[.]com
- hpesystem[.]com
- cybersecnet[.]org
- cybersecnet[.]co[.]za
- excsrvcdn[.]com
- online-analytic[.]com
- web-traffic[.]info
- hpesystem[.]com
- indianmombais[.]com
- defenderstatus[.]com
- zonestatistic[.]com

The following domains were identified during the course of analysis; the joint team assesses that these domains are likely associated with Lyceum as part of its past or current infrastructure.

- checkinternet[.]org
- digitalmarketingagency[.]net
- dnsanalyzer[.]com
- livednscdn[.]com
- microsoftonline[.]net

The following Lyceum domains were seen to be used by the reconfigured or new Lyceum backdoor:

- centosupdatecdn[.]com
- dnscatalog[.]net
- securednsservice[.]net
- uctpostgraduate[.]com

For reference and further analysis, defenders can access the following file-hashes related to the Milan and Shark backdoors:

Shark:

```
89ab99f5721b691e5513f4192e7c96eb0981ddb6c2d2b94c1a32e2df896397b82f2ef9e3f6db2146
bd277d3c4e94c002ecaf7deaabafe6195fddabc81a8ee76c44faf11719b3a679e7a6dd5db40033ec4
dd6e1b0361c145b81586cb735a64112f6ae4f4373510c4e096fab84383b547c8997ccf3673c00660
df8a3dc9ed1f3ca
```

Milan:

```
B46949feeda8726c0fb86d3cd32d3f3f53f6d2e6e3fcd6f893a76b8b2632b249d3606e2e36db0a0cb1
b8168423188ee66332cae24fe59d63f93f5f53ab7c302921ab4357262993a042c28c1cdb52b2dab71
95a6c30fa8be723631604dd330b29a2754d7995426b58317e437f8ed6770cd7bb7b18d971e23b2b30
0b75e34fa086b766522dd4189fef7775d663e5649ba9d8be8e03022039d20848fcbcb3643e5f2b54a67
062bdcd32dfa9f3d7b69780d2e6e4925777290bc34e8f979a1b4b72ea2
```

Detailed Technical Description:

ACTI/PACT will only provide a brief presentation of the malware families and will focus on the C2 communication aspects that analysts observed in Prevailion's telemetry, since ClearSky and Kaspersky have already provided detailed technical descriptions of the Shark and Milan (a.k.a. James) backdoors.

Shark:

Shark is a 32-bit executable written in C# and .NET. To run Shark, a parameter is passed on the command line that includes the executable's filename. Shark generates a mutex that uses the executable's filename as the mutex value. The mutex likely ensures Shark does not execute on a machine where it is already running and that the correct version of Shark is executed.

Shark does not use code to facilitate persistence; instead, Shark runs its functions as infinite threads, which enables Shark to persist as long as the victim's machine is turned on. The developers likely designed Shark for clients or servers with high uptime or for machines to which they have access and can re-launch the Shark executable if the machine is turned off.

Shark uses a function called "redus" to produce a configuration file that is XOR-encoded, compressed with Gzip, and has the same name as the Shark executable. All files that ACTI analyzed were XOR-encoded with the hexadecimal key 0x2a.

```
S1:zonestatistic.com
S2:zonestatistic.com
T1:30
T2:30
d1:c:\users\luke\desktop\winlangdbdir\468526d1102461
u1:c:\users\luke\desktop\winlangdbdir\572096u1696995
d2:c:\users\luke\desktop\winlangdbdir\455639d2404786
u2:c:\users\luke\desktop\winlangdbdir\366213u2391297
id:3c73c359
sh:8
di:5
hi:5
HS:1
```

Image 1: Snip from Shark Configuration File

The configuration file contains at least one C2 domain, which is used with a DGA for DNS tunneling or HTTP C2 communications. The C2 domains' authoritative name server is attacker-controlled, allowing Lyceum operators to provide commands through IP addresses in the A records of DNS responses.

Specific parameters within the Shark backdoor configuration file indicate whether the backdoor is to use DNS or HTTP for C2:

- S1, S2: The configured C2 servers.
- T1, T2: Sleep time values.

Some of the Milan backdoors analyzed by ACTI also include samples that were clustered as DanBot backdoors in ClearSky's report. However, these samples are all written in Visual C++ and .NET, while DanBot samples are written in C# and .NET. Although there are certain differences among the Milan samples, ACTI has conducted sample comparisons indicating a high similarity across this cluster of Milan samples. The image below depicts five Milan samples in which the strings in each sample has a greater than 86% code similarity rate with the other backdoors.



Image 3: Sample Similarity Coverings Functions and strings among Milan Samples

Like Shark, Milan queries the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid` to retrieve the GUID for the victim machine, from which both backdoors use the last eight characters to generate a unique identifier for the victim machine.

Like Shark, Milan is also able to use both DNS and HTTP(S) for C2 communications. For C2 communications over DNS, Milan uses hardcoded domains as the input for a custom (DGA). The DGA is documented in Kaspersky's report as is some of the syntax used by Milan for C2 over HTTP(S).

However, ACTI found that some of the legacy Milan backdoors retrieve data by generating requests using the hard-coded domain and then requesting one of a number Active Server Page-related URL paths. These URL paths are hardcoded within some of the Milan samples. Those identified by ACTI were:

- `contact.aspx`
- `default.aspx`
- `preview.aspx`
- `team.aspx`

ACTI/PACT Investigation:

ACTI started seeing the Shark campaign in host-based telemetry on July 19, 2021, when various hosts in Israel started executing a Shark backdoor with the following attributes:

Filename: "Shark.exe"

SHA-256: 2f2ef9e3f6db2146bd277d3c4e94c002ecaf7deaabafe6195fddabc81a8ee76c

ACTI observed this file being executed on a large number of hosts in Israel. Many of these machines carried Windows 10 Enterprise and Pro builds, while other observed operating systems within victim environments were older Windows Server 2016 Datacenter and Windows Server 2019 Datacenter builds. It is possible that some of the machines executing Shark.exe were part of an incident response effort – against the Lyceum campaigns – as they appear to have operating systems within (likely multiple individual) virtual machines that appear to have been created for single executions of the Shark backdoor on a variety of Windows operating systems. The referenced file (Shark.exe) was first submitted to a third-party malware repository on August 2, 2021 from a submitter who appears to be based in Israel. On September 27, 2021, the same third-party malware repository submitter also uploaded a file with the following attributes:

Filename: "data.dat"

SHA-256: 17ab5ee10033da8a519c0547581f40677b973345d8c3172a4fde612692188460

This file is not malicious but contains the output from DNS requests generated by the DGA and the hardcoded C2 domain in the previously referenced Shark.exe file.



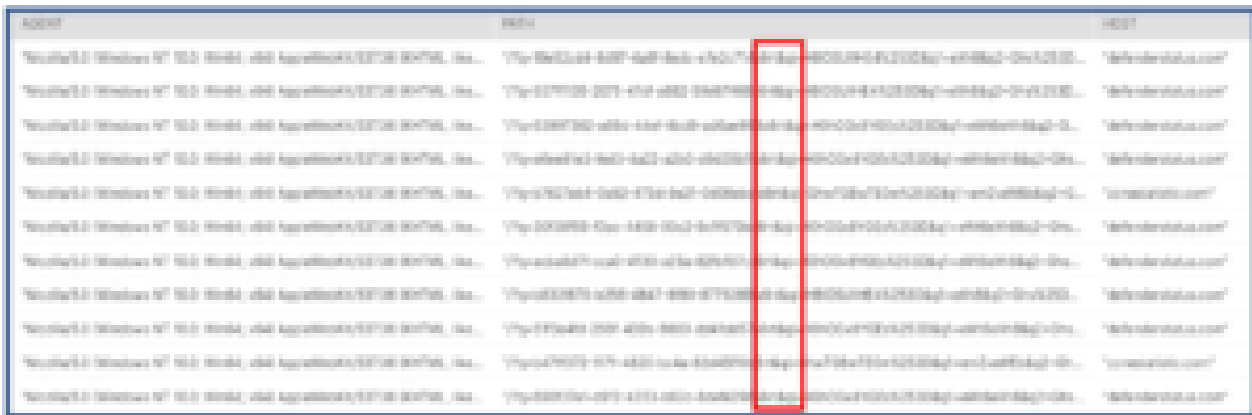
```
3135257432333132.defenderstatus.com
3135257432343136.defenderstatus.com
3135257432353230.defenderstatus.com
3135257432363234.defenderstatus.com
6370782574323730.defenderstatus.com
6370782574323834.defenderstatus.com
6370782574333038.defenderstatus.com
637078257433313132.defenderstatus.com
637078257433323136.defenderstatus.com
637078257433333230.defenderstatus.com
637078257433343234.defenderstatus.com
637078257433343238.defenderstatus.com
```

Image 4: Shark Generated Subdomains Found in File Uploaded from Israel

Seen in totality, the host-based Shark executions coupled with Shark backdoor and telemetry submissions from Israel, indicated to the ACTI/PACT research team that victimology would likely include Lyceum victims in Israel. The research team overlaid the Shark malware syntax on the Prevailion's C2 telemetry, which at the time of analysis consisted of data from 14 assessed Lyceum C2 domains. This was initially done to detect DGA-generated DNS requests and subsequently the previously described HTTP patterns. The effort focusing on

Shark-generated DNS requests only yielded what is assessed to be sandbox runs of Shark samples, egressing from various IP-address infrastructure owned by security or cloud vendors.

However, when the ACTI/PACT research team queried the Prevaillon dataset based on the previously referenced regular expression, consistent beaconing was observed through September and continuing into October 2021 from a number of IP addresses resolving to telecommunication companies and ISPs in Israel and Saudi Arabia. The inclusion of the parameter: “s6rt” (see red box in image below) indicate backdoors where traffic was set for beaconing.



AGENT	URL	HOST
Windows 10 21H2, x64, Architecture: x64,s6rt...defenderstatus.com	defenderstatus.com
Windows 10 21H2, x64, Architecture: x64,s6rt...defenderstatus.com	defenderstatus.com
Windows 10 21H2, x64, Architecture: x64,s6rt...defenderstatus.com	defenderstatus.com
Windows 10 21H2, x64, Architecture: x64,s6rt...defenderstatus.com	defenderstatus.com
Windows 10 21H2, x64, Architecture: x64,s6rt...defenderstatus.com	defenderstatus.com
Windows 10 21H2, x64, Architecture: x64,s6rt...defenderstatus.com	defenderstatus.com
Windows 10 21H2, x64, Architecture: x64,s6rt...defenderstatus.com	defenderstatus.com
Windows 10 21H2, x64, Architecture: x64,s6rt...defenderstatus.com	defenderstatus.com
Windows 10 21H2, x64, Architecture: x64,s6rt...defenderstatus.com	defenderstatus.com
Windows 10 21H2, x64, Architecture: x64,s6rt...defenderstatus.com	defenderstatus.com
Windows 10 21H2, x64, Architecture: x64,s6rt...defenderstatus.com	defenderstatus.com

Image 5: Prevaillon Telemetry Indicating Backdoor Activity Egressing from Shark Backdoor Victims

The Shark backdoors were likely in beacon mode due to Lyceum operators having lost control of the backdoor following Prevaillon’s assumption of control of the Shark C2 domains: “defenderstatus[.]com” and “zonestatistic[.]com”

Queries for a DGA generated by the Milan backdoor yielded the same kind of telemetry as seen for the Shark DGA-generated DNS requests. As with Shark, most of them were short duration beacons egressing from cloud or IP spaces related to security vendors. The lack of use of the DGA DNS tunneling in the observed Lyceum C2 telemetry could indicate that the DNS tunnelling is only used during the first phase of the compromise, but then retired in preference of HTTP(S) as Lyceum becomes well established in the victim network.

When the ACTI/PACT team queried the Prevaillon dataset for the previously referenced known hardcoded URL paths contact.aspx, Default.aspx, preview.aspx, and team.aspx observed in Milan samples, the researchers observed continued beaconing from an IP address that resolved to a telecommunications operator in Morocco.

"indiamombais.com"	"Mozilla/5.0 (Windows NT 7.1; WOW64; rv:32.0) Gecko/20100104 Firefox/52.0"	"default.asp"
"indiamombais.com"	"Mozilla/5.0 (Windows NT 7.1; WOW64; rv:32.0) Gecko/20100104 Firefox/52.0"	"default.asp"
"indiamombais.com"	"Mozilla/5.0 (Windows NT 7.1; WOW64; rv:32.0) Gecko/20100104 Firefox/52.0"	"default.asp"

Image 6: Prevailion Telemetry Indicating Backdoor Activity Egressing from MilanRAT Backdoor Victims

It is unknown if the Milan backdoor beacons are coming from a customer of the Moroccan telecommunication operator or from internal systems within the operator. However, since Lyceum has historically targeted telecommunication providers and the Kaspersky team identified recent targeting of telecommunication operators in Tunisia, it would follow that Lyceum is targeting other north African telecommunication companies. The ACTI/PACT research team therefore assess that the observed Milan activity is likely emanating directly from within the Moroccan telecommunications operator.

During late October 2021 the ACTI/PACT team identified beaconing from a reconfigured or possibly a new Lyceum backdoor. The observed beacons looked like the following:

```

/?index=3&serv=MDAANDEONrcwCpRB
/?proto=6&index=OTM3NDdFYU4MDOyNDdmMjZyaFmQWVjOGZhdMzkwOTY%3D
/?index=3&serv=MDAANDEONrcwCpRB
/?proto=6&index=OTM3NDdFYU4MDOyNDdmMjZyaFmQWVjOGZhdMzkwOTY%3D
/?proto=6&index=OTM3NDdFYU4MDOyNDdmMjZyaFmQWVjOGZhdMzkwOTY%3D&name=LnNlY3VyZWZluc3RlcwZyY3LubemV0
/?proto=3&index=MDAANDEONrcwCpRB
/?proto=6&index=MDAANDEONrcwCpRB&name=Lmlluc2NhdGFsZ3cubemV0
/?proto=6&index=MDAANDEONrcwCpRB&name=Lmlluc2NhdGFsZ3cubemV0
/?proto=6&index=MDAANDEONrcwCpRB&name=Lmlluc2NhdGFsZ3cubemV0
/?proto=2&index=MDAANDEONrcwCpRB
/?proto=2&index=MDAANDEONrcwCpRB
/?proto=6&index=OTM3NDdFYU4MDOyNDdmMjZyaFmQWVjOGZhdMzkwOTY%3D&name=LnNlY3VyZWZluc3RlcwZyY3LubemV0
/?proto=3&index=OTM3NDdFYU4MDOyNDdmMjZyaFmQWVjOGZhdMzkwOTY%3D
/?proto=3&index=OTM3NDdFYU4MDOyNDdmMjZyaFmQWVjOGZhdMzkwOTY%3D
/?proto=3&index=OTM3NDdFYU4MDOyNDdmMjZyaFmQWVjOGZhdMzkwOTY%3D
/?proto=6&index=OTM3NDdFYU4MDOyNDdmMjZyaFmQWVjOGZhdMzkwOTY%3D&name=LnNlY3VyZWZluc3RlcwZyY3LubemV0
/?proto=6&index=OTM3NDdFYU4MDOyNDdmMjZyaFmQWVjOGZhdMzkwOTY%3D&name=LnNlY3VyZWZluc3RlcwZyY3LubemV0
/?proto=6&api=5nQvVEEdDQeG0&name=Lmlluc2NhdGFsZ3cubemV0
/?proto=3&api=5nQvVEEdDQeG0

```

Image 7: Observed Beaconing from a Reconfigured or New Lyceum Backdoor

The observed beacons were seen egressing from a telecommunications company in Tunisia as well as an MFA in Africa. The URL syntax of the newly reconfigured backdoor are somewhat similar to those generated in the newer version of Milan.

```

https://akastatus[.]com/?id=iCIG4F0fzf&formid=M2M3M2MzNTk%3d1111111i1
https://securednsservice[.]net/?
proto=6&index=MjYkYzEwZWY5NTY5NDk3ZDg2YTljNDYzNWQxYTc0YTM%3D&name=

```

The URL syntax is configurable within the Milan backdoor and ACTI/PACT assesses it as likely that the Lyceum operators reconfigured the URL syntax used by Milan to circumvent IDS or IPS that were encoded to detect previous the Milan beacon syntax. The new backdoor syntax is matched by the following regular expression:

```
/?(proto|kind|pt)=[0-9]{1}&(index|pi|serv)=/
```

However, as it is configurable it may only be useful to create ad-hoc network detection rules.

ACTI provides actionable and relevant threat intelligence to support decision makers. More information on this activity is available to subscribed ACTI IntelGraph customers. IntelGraph is a proprietary next-generation security intelligence platform that allows users to search, visualize, and contextualize the relationships among malicious actors, their tools, and the vulnerabilities they exploit.

Accenture Security helps organizations build resilience from the inside out so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture helps organizations protect their valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit us at www.accenture.com/security.

Accenture, the Accenture logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of Accenture and its subsidiaries in the United States and in foreign countries. All trademarks are properties of their respective owners. All materials are intended for the original recipient only. The reproduction and distribution of this material is forbidden without express written permission from Accenture. The opinions, statements, and assessments in this report are solely those of the individual author(s) and do not constitute legal advice, nor do they necessarily reflect the views of Accenture, its subsidiaries, or affiliates. Given the inherent nature of threat intelligence, the content contained in this report is based on information gathered and understood at the time of its creation. It is subject to change. Accenture provides the information on an “as-is” basis without representation or warranty and accepts no liability for any action or failure to act taken in response to the information contained or referenced in this report.

This document makes reference to marks owned by third parties. All such third-party marks are the property of their respective owners. No sponsorship, endorsement or approval of this content by the owners of such marks is intended, expressed or implied.

Copyright © 2021 Accenture. All rights reserved.