RoboSki and global recovery: Automation to combat evolving obfuscation

Light Dark

July 12, 2021

By Melissa Frydrych, Claire Zaboeva, Dan Dash

12 min read

Advanced Threats Malware Risk Management Security Services Threat Hunting Threat Intelligence

In a recent collaboration to investigate a rise in malware infections featuring a commercial remote access trojan (RAT), IBM Security X-Force and Cipher Tech Solutions (CT), a defense and intelligence security firm, investigated malicious activity that spiked in the first quarter of 2021. With over 1,300 malware samples collected, the teams analyzed the delivery of a new variant of the RoboSki packer, which is widely used to thwart detection and deliver commodity RATs to enterprise networks.

CT automated the capability to rapidly extract configuration data from malware to produce actionable indicators of compromise (IOCs). Analysts tested the ability to statically extract configuration data, bypassing dynamic anti-analysis features using data processed by CT, discovering approximately 1,300 additional samples. The RoboSki-packed malware samples feature new capabilities, such as the ability to load resources and convert pixelated data to RGB order, resulting in the RoboSki component, and decoding and decrypting a ReZer0 loader. The ReZer0 loader can embed malware or fetch it from remote servers and is known for its ability to deliver encrypted payloads and anti-sandbox checks. Layering loaders is a tactic many malware distributors use to evade anti-virus detection and security scanners.

CT partnered with IBM X-Force to uncover how attackers delivered the commercial RATs. While analyzing the delivery of RoboSki samples, X-Force isolated a sample of 21 phishing emails addressed to organizations worldwide in and around mid-February 2021 with attachments including RoboSki-packed malware. The emails, which feature global trade themes, lead to the delivery of malware, such as Agent Tesla, FormBook, njRAT, NetWire and the Remcos RAT. X-Force found infrastructure overlaps with the delivery of RoboSki's distribution and recent or ongoing activity spreading malware such as AsyncRAT, LokiBot, NanoCore and the Gamarue Botnet, in addition to Agent Tesla, FormBook, njRAT, NanoCore and Remcos RAT, which have previously been reported on IBM's premium threat intelligence platform TruSTAR and Security Intelligence.

attribute the new RoboSki variant analyzed, or its means of delivery, exclusively to Vendetta. The teams believe that the activity points to independent cyber criminals distributing malware globally as part of a continuous effort to evolve tools and methods, obfuscate activity and evade detection.

Are cyber criminals riding the tide of global recovery?

Last year saw the global economy experience the worst peacetime economic decline since the Great Depression, but in its economic growth forecast for 2021, the International Monetary Fund predicts renewed global economic expansion of 6% in 2021. Arguably underpinning this recovery in global trade is a worldwide expansion in the e-commerce ecosystem, which grew by a staggering 30% within the last year. Doubtlessly attune to these changes in the digital current, malicious cyber actors are baiting their hooks to imitate authentic requests for quotations, payment orders and shipping updates, hoping to snare those logistics linchpins, like manufacturers, shippers and suppliers, in the global supply chain.

X-Force analysts studied a sample of 21 phishing emails containing malicious attachments that deliver the RoboSki packer and subsequently a variety of final payloads. Analyzed emails were sent between the second and third week of February 2021 and were categorized into three main themes: purchase order/request for quotation/inquiry, shipping notification and payment notice/bank transfers. The sample emails were sent to 15 unique companies located in 12 different countries across Europe, South America, the Middle East and South Asia.

In all instances, the phishing emails were addressed to companies associated with the manufacture or export of items supporting and/or supplying construction, transport, engineering or energy services. Most samples were directed at entities in Europe, with the highest concentration of targeted organizations based in Romania, Italy and Germany.

X-Force and CT analysts assessed with high confidence that global trade- and logistics-themed phishing campaigns will continue to plague

should exercise extra caution and seek to cultivate a culture of cyber awareness among management and employees.

New orders and requests for quotations

Most emails in the sample were sent to a Romania-based company characterized as a global supplier of electrotechnical power products, including power transformers and rotary electric machines. Several of the emails were crafted to appear to originate from real company email domains, indicating the senders are trying to increase the likelihood that the phishing email appears legitimate. Apart from a single instance, the emails pose as an inquiry for purchase orders and requests for quotations. All emails are written in poor English and include an attached purchase order or quotation contained in an archive file (Zip, CAB or RAR), which, when executed, drops the RoboSki-packed malware.

Figure 1: Sample email sent to a Romania-based company

Additional phishing messages uncovered with the same theme were composed in varying qualities of English and directed at seven unique

the quality of the text differs by sample, the uncovered emails contain signature blocks attempting to impersonate well-known global corporations.

Where's my package?

The teams found the email sender janattbs7[@]gmail[.]com sent not only an email to the Romanian-based company regarding a "quotation request," but also an email for "shipping documents." Due to additional emails sent to the same company with varying themes, X-Force researched the spoofed sender company as well as the recipient company; however, no clear connection between the two was discerned.

Some of the sample emails used package delivery lures that purported to come from DHL or FedEx. These were typically sent to companies within the construction industry that support oil companies and government clients, as well as water technology and processing.

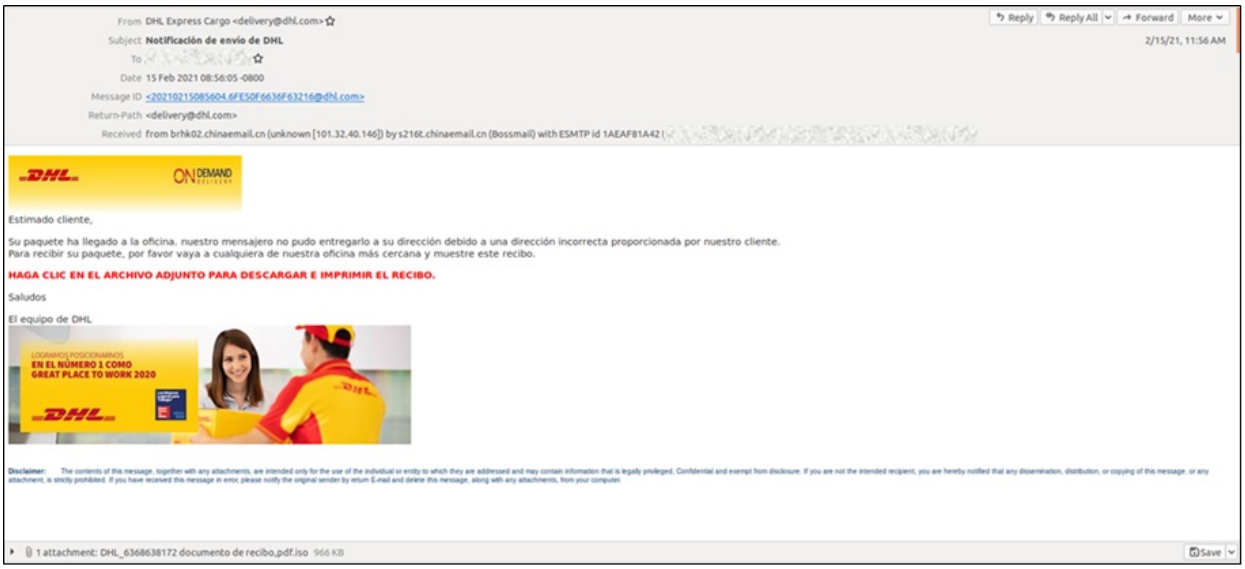


Figure 2: Sample DHL email

"Dear Customer,

Your package has arrived at the office. Our courier could not deliver it to your address due to a wrong address provided by our customer.

To receive your package, please go to any of our nearest office and show this receipt.

Greetings

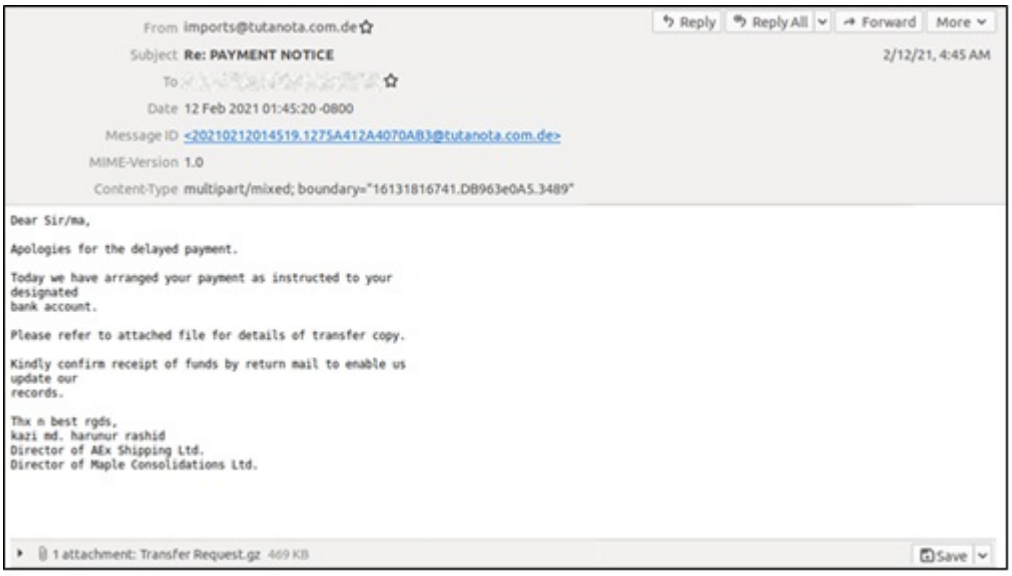
The DHL team”

Fake notices, payments and invoices

Other emails in the sample featured fake payment notices, invoices or bank transfers and were sent to organizations in Europe and the Middle East. Half of the samples were composed in the native language of the targeted recipients and contained signature blocks of authentic banks or import/export companies. The remaining emails were composed in well-written English and featured signature blocks impersonating the managing director of a legitimate global shipping and logistics/supply chain management company based in Bangladesh.

While the sender email addresses did not match the signature blocks featured in each of the samples, in all cases the signature blocks themselves imitated authentic companies that may have a legitimate interest in the products or services of the targeted corporation.

In two instances, emails used the encrypted email service Tutanota (ex. imports[@]tutanota[.]com[.]de.). Affixed to each of these emails was an attached archive file (TAR, 7z, GZIP) posing as either transfer requests, SWIFT statements from an authentic bank or numeric codes potentially pointing to account numbers.



Observations from X-Force's analysis

X-Force uncovered several unique characteristics that provide insight into the attack infrastructure used in the various delivery of RoboSki-packed malware to facilitate operations. The activity examined involved at least 289 email addresses for exfiltration, of which about 150 do not appear legitimate nor have discoverable returns, while more than half appear to be valid accounts.

About 20% of the valid email accounts showed server errors, and roughly 10% of accounts were associated with catch-all servers that accept emails sent to the domain, regardless of whether the mailbox exists or not. The remaining accounts returned as either belonging to invalid domains with no mail exchange record, bad syntax, transient network faults or unknown status.

Infrastructure overlaps with distribution of other malware

The researchers isolated about 165 different command and control (C2) IP addresses and domains that were used in the distribution of malicious payloads. Several IP addresses and domains have been reported in previous malware campaigns or are associated with recent or ongoing activity delivering a variety of other malware. Some malware variants include Eldorado, Telegram Bot, NanoBot, LokiBot and the password stealers Fareit and Redline. The following represents a sample of the recent or ongoing campaigns that share or have shared infrastructure overlaps with the RoboSki packer.

AsyncRAT

Some malicious overlaps include domain 8123wsheurope.access[.]ly, which resolved to the RoboSki-packed AsyncRAT C2 IP address 79.134.225[.]44 in December 2020. Recently, this domain was reported as being part of activity in which attackers used collaboration platforms, such as Slack, to evade detection and deliver several types of RATs and stealers. AsyncRAT has also

NanoCore RAT

In the same netblock as the AsyncRAT IP address, a RoboSki-packed NanoCore C2 IP address 79.134.225[.]71 resolved to adam9.ddns[.]net, which was a C2 domain reported in late 2020 with relation to activities by the Blade Eagle (Blade Hawk) advanced persistent threat (APT) group. In that campaign, Blade Eagle targeted organizations in the Middle East and West Asia. We also found that C2 domains uyeco[.]pw and zolta[.]icu were seen in a recent malspam campaign in which malicious executable file formats were abused and used in a way that hid them from email scanners and anti-malware software, ultimately to deliver the NanoCore RAT. The infection tactics, techniques and procedures (TTPs) were similar to the ones used to deliver the RoboSki-packed malware, via emails themed with purchase orders in archived files.

LokiBot

Other observed overlaps include RoboSki-packed LokiBot C2 domains:

Click and scroll to view full table

These were previously observed in a campaign using Microsoft Publisher files to deliver the Pony malware. The domains were also reported as a separate phishing campaign in 2019 using 'SWIFT monetary transfer' themed lures to deliver LokiBot, in addition to Neshta and Fuerboos. All four C2 domains were used again in October 2020, as part of a different Lokibot spam campaign. Of note, these C2 domains were present in 95 of the RoboSki-packed LokiBot samples, accounting for 41 unique LokiBot payloads.

Gamarue Botnet

In addition, the C2 domains azmtool[.]us, becharnise[.]ir, newcesarnex[.]com and klimsourcinq[.]com were reported in February as being related to the

File path observations

Some file paths have noticeable misspellings, such as %AppData%\microsift.exe, which was observed in a RoboSki-packed AsyncRAT sample. We found that additional file paths, such as %Temp%\windefendllinici.exe in RoboSki-packed AsyncRAT samples, may be associated with files compiled in February 2021 that matched YARA signatures for Nanocore, and password stealers, several of which communicate with the RoboSki-packed AsyncRAT C2 domain laboratoriogenfarp.linkpc[.]net.

It is possible the appearance of the same file path in a limited sample set may suggest that the same malicious actor has been involved in several campaigns delivering various malware. File path %AppData%\notes\logs.dat, seen in a RoboSki-packed Remcos sample, was also observed within other files that matched YARA rules for Remcos RAT and Agent Tesla. The presence of %AppData%\seguridad\logs.dat in a RoboSki-packed Remcos sample may suggest that a Spanish-speaking company may have had their security logs accessed. In addition, this file path was found within a file possibly related to Razy malware.

License re-use

While analyzing some of the final payloads, some interesting and specific attributes regarding Remcos RAT were observed. Analysts found that the Remcos configuration contains a license code field ('license_code'), which is unique to each purchaser. In some cases where the RoboSki packer led to the delivery of Remcos, it was observed that two specific license codes were re-used.

The license codes observed within the configuration of multiple payloads for packaging were:

1. License code A830299B3222E31F1F2765E3AC4D37FD was observed four times and associated with C2 addresses 184.140.53.148:1011

eight instances, associated with C2 addresses 91.241.19.107:1313 and 176.111.174.14:2804.

In addition, the configuration of Remcos RAT contains the field 'server_password,' with both of these license codes using the password 'Yes'— although it is possibly defined as the default password.

New RoboSki version — The technical details

As identified by X-Force, the RoboSki packer file typically arrives within a malicious email archive attachment. CT further analyzed the packer and its embedded components to understand the execution flow leading to a commodity RAT payload and how that execution flow differed from previous RoboSki packers.

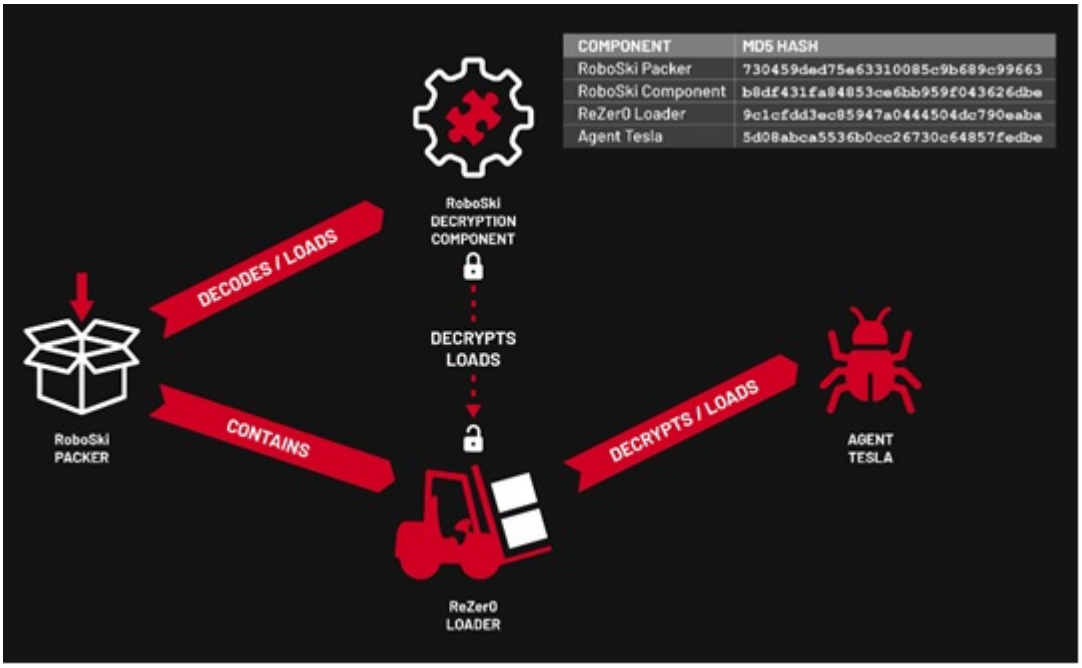


Figure 4: Mapping of RoboSki packer to final payload

RoboSki.Packer

CT analysts found that the RoboSki packer contains numerous .NET Microsoft resources, including the two resources of interest, SzGeneric and

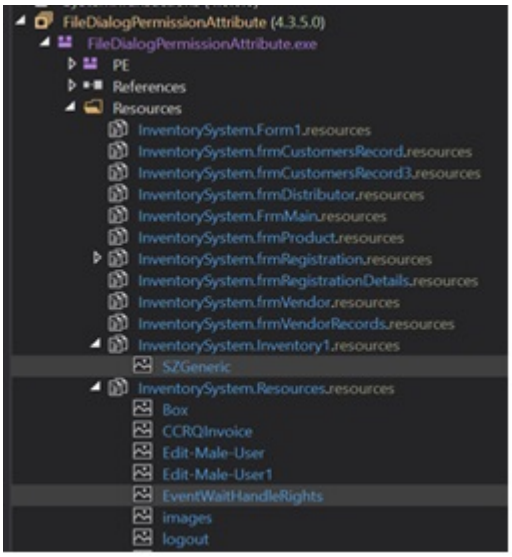


Figure 5: Key resources

The resource SzGeneric contains the RoboSki component, which is used to decrypt the contents of the resource EventWaitHandleRights, resulting in a ReZer0 loader. To get to the ReZer0 loader, the RoboSki packer first loads the SzGeneric resource and converts the pixel data to RGB order, as denoted in the image below, resulting in the RoboSki component.

Figure 6: Conversion to RGB order

This differs from previous RoboSki packer versions, wherein the component was stored as string data and decoded using string replacement and the Base32 algorithm or string replacement, string reversal and the Base64 algorithm.

The converted data is then executed and invoked in a series of module calls, depicted in the image below, in which the component is executed from its

Figure 7: Converted data executed and invoked

The parameters stored within ChannelSinkStack are the hex-encoded values for the resource named EventWaitHandleRights and a base XOR key ‘xNksm.’

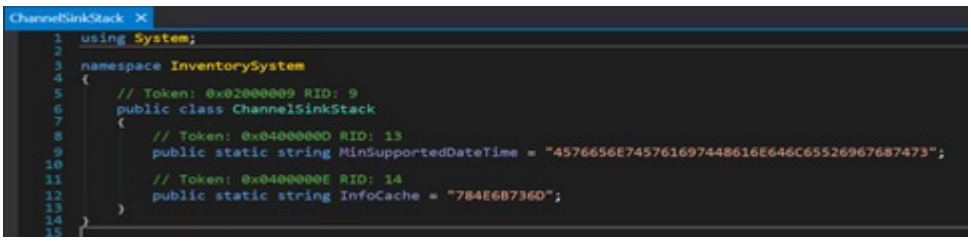


Figure 8: ChannelSinkStack parameters

RoboSki.Component

As described above, during execution the RoboSki component is provided as a resource and XOR key parameters, and proceeds to decode and decrypt the ReZer0 loader from the RoboSki packer. The component loads the resource and arranges the pixels in BGRA order. The component then parses the resource according to the structure below, and XOR decrypts the data using the results of permutations against the base XOR key and a control key.

```
PAYLOAD_SPEC = construct.Struct(
    "size" / construct.Int32ul,
    "encrypted" / construct.Bytes(this.size - 1),
    "control_key" / construct.Bytes(1)
)
```

Figure 9: Python construct library structure

Figure 10: Structure parsing and XOR decryption

The resultant ReZer0 loader is then executed in memory and subsequently decrypts and executes an embedded payload, which, in this case, is an instance of the Agent Tesla RAT. The ReZer0 loader operates in the same manner as described by 360 Total Security and Fortinet. As mentioned in those blog posts, the ReZer0 loader exhibits anti-analysis features such as detection of virtual machines or sandboxes and can bypass anti-virus software. Due to these anti-analysis features, the results from dynamic analysis, including sandboxes, may be incomplete or wildly inaccurate. By using automated component and configuration extraction (ACCE) to statically extract the configuration data, the researchers bypassed all dynamic anti-analysis features that would otherwise prevent accurate and reliable analysis.

How is ACCE support built?

ACCE is built on top of CT's proprietary libraries, as well as the Department of Defense Cyber Crime Center's (DC3) malware configuration parser and kordesii frameworks. This promotes an automation workflow where initial YARA signature detections prompt running targeted modules organized by capability to extract layers of components (RoboSki packer-> ReZer0 loader -> Agent Tesla payload) and report configuration at each layer. By adopting the ACCE workflow, reverse engineers can develop modules based upon analysis of a few samples, and then leverage that module to extract results from thousands of other related malware variants.

Previously, written code for parsing the PNG pixels of the image resource was used in conjunction with new code for obtaining and using the resource name and initial XOR key using construct, regex patterns and an internal library.

```
SPEC = construct.Struct(
    "cfg_re" / construct.Select(
        construct.Regex(
            re.compile(
                # 730459ded75e63310085c9b689c99663 @ 0x00000650
                br"""
                    \x72(?P<rn>.{3})\x70)    # ldstr    HEX_ENC_RSRC_NAME
                    \x80.{3}\x04             # stsfld   string Lion_Match_Employee_Management_System.Channel
                    \x72(?P<kb>.{3})\x70)    # ldstr    HEX_ENC_KEY
                    \x80.{3}\x04             # stsfld   string Lion_Match_Employee_Management_System.Channel
                    \x2a                     # ret
                """,
                re.DOTALL | re.VERBOSE
            ),
            rn=dotnetfile.DotNetString(construct.Int32ul), kb=dotnetfile.DotNetString(construct.Int32ul)
        ),
```

Figure 11: Construct

```
    img_data = self.get_rsrc_img_data(data, name)
    if not img_data:
        return
    logger.info(f"Attempting to ARGB decode and XOR decrypt the data in .NET resource {name}.")
    png_data = image_pixel.parse_png_pixels(img_data, name, "BGRA")
    try:
        info = self.PAYLOAD_SPEC.parse(png_data)
    except construct.ConstructError:
        logger.warning(
            f"The method in which .NET resource {name} is encoded/encrypted could not be determined. Outputting "
            f"the resource data for manual review."
        )
        self.reporter.output_file(png_data, name, "Encrypted Payload Structure")
    else:
        key_xor = ctcipher.new("xor", info.control_key)
        init_key = key_xor.decrypt(base_key)
        init_xor = ctcipher.new("xor", init_key)
        encrypted = init_xor.decrypt(info.encrypted)
```

Figure 12: Construct PAYLOAD_SPEC

The referenced resource is acquired, PNG pixels are parsed and the resulting data is parsed using the construct PAYLOAD_SPEC.

Subsequently, the ReZer0 loader is decrypted and dispatched for further processing. The configuration output for the RoboSki packer (MD5: 9b792353406c1c8bf440fa5417aee5b2), which contained the LokiBot sample with C2 domains previously observed in other campaigns.

```
c2_url:
- http://51.195.53.221/p.php/oiBqOp4YvDjmf
- http://kbfvzoboss.bid/alien/fre.php
- http://alphastand.trade/alien/fre.php
- http://alphastand.win/alien/fre.php
- http://alphastand.top/alien/fre.php
key:
- '0x5720570657'
- '0x63f828fe6298fb639b27d4849882be471b9162900bf49563ad27acded2fad70d75f80
- '0xf86af04da7d691e6be98fd3db48b9b7b3779389495f95125'
other:
  base_xor_key: '0x0077005100'
  tdes_iv: '0x4cf8799b5abda2c0'
  tdes_key: '0xf86af04da7d691e6be98fd3db48b9b7b3779389495f95125'
  tdes_key_iv: 0xf86af04da7d691e6be98fd3db48b9b7b3779389495f95125:0x4cf879
  xor_key:
  - '0x5720570657'
  - '0x63f828fe6298fb639b27d4849882be471b9162900bf49563ad27acded2fad70d75f
outputfile:
- - b8df431fa84853ce6bb959f043626dbe_x86.dll
  - RoboSki Decryptor Component (XOR)
  - b8df431fa84853ce6bb959f043626dbe
- - c0e512bfc316ec926a56e4dd31258875_x86.dll
  - ReZer0 Loader (XOR Resource)
  - c0e512bfc316ec926a56e4dd31258875
- - 9064120cc16a90f4c6fe4a9cda3eeb82_x86.exe
  - LokiBot Implant
  - 9064120cc16a90f4c6fe4a9cda3eeb82
```

Figure 13: Configuration output

Threat hunting using ACCE output

After adding a parser module to automatically extract the RoboSki component and ReZer0 loader from the new RoboSki packer variant, the researchers used VirusTotal to find additional samples using the new RoboSki packer variant. As a result, 55 samples were selected to test against the new parser module.

Two variations in the initial RoboSki packer were observed:

1. In addition to being hex-encoded, the .NET Microsoft resource name and base XOR key are Base64 encoded.
2. A .NET obfuscator is leveraged to encrypt all strings in the RoboSki packer, inhibiting the ability to easily extract the resource name and base XOR key.

After updating the parser module(s) to support the variations observed in the RoboSki packer, approximately 1,300 additional RoboSki packer samples were obtained via VirusTotal and subsequently run against the capability. The resultant payload distribution is as denoted in the following chart:

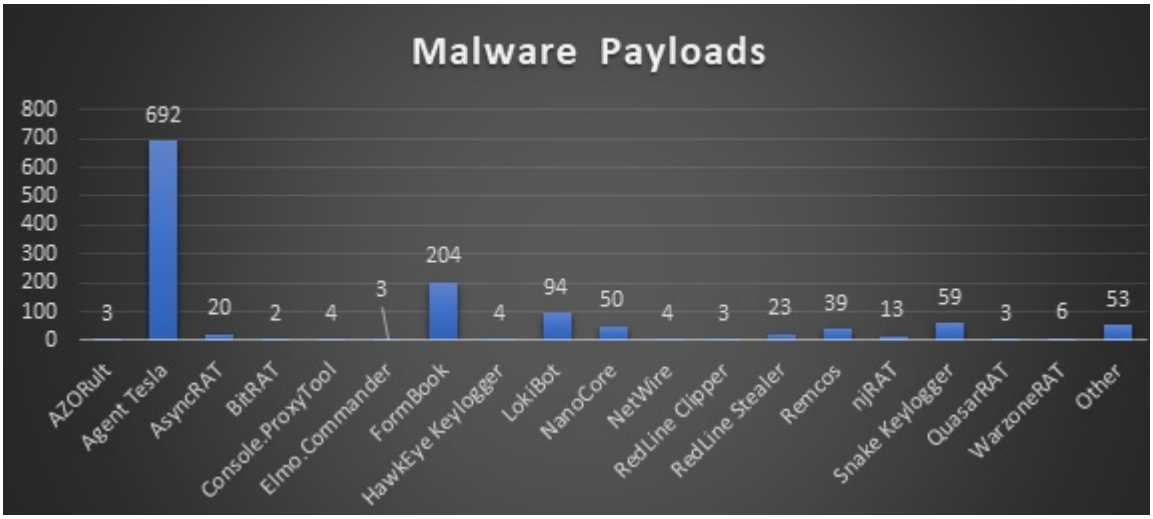


Figure 14: Payload distribution

The most common payload observed was Agent Tesla, accounting for over half of the obtained payloads. Notably, all the payloads fell into a category of commodity malware such as information stealers or commercial RATs.

An ever-evolving commodity malware scene

Malware distribution is a continually evolving practice undertaken by potential botnet herders and spam distributors alike, constantly on the quest to bypass organizational security controls to deliver malware. As part of that ecosystem, commodity packers, such as RoboSki, are used extensively to spread numerous types of malicious code. Keeping up to date about new variations, IOCs and overall delivery TTPs are essential to keeping networks free of malware that could eventually result in more advanced compromises.

To avoid the associated risks that come with a reliance on digital exchange for operations, the use of automation to rapidly generate indicators can help equip net defenders with the necessary insight to identify and prevent compromise. X-Force and CT analysts assess with high confidence that the

import and export of items worldwide should exercise extreme caution and harden their network environments.

For up-to-date information about malware campaigns, IOCs and malware reports, join us on X-Force Exchange.

IBM X-Force Research | shipping | Advanced Malware | Malware | Obfuscation | Remote Access Tools (RATs) | Remote-Access Trojan (RAT) | X-Force

Melissa Frydrych
Threat Hunt Researcher, IBM

Claire Zaboeva
Senior Strategic Cyber Threat Analyst, IBM

Dan Dash
Reverse Engineer, Cipher Tech Solutions

POPULAR