Aug 09 2024

NETMANAGEIT

Intelligence Report

Threat actor targeting UK banks in ongoing AnyDesk social engineering campaign

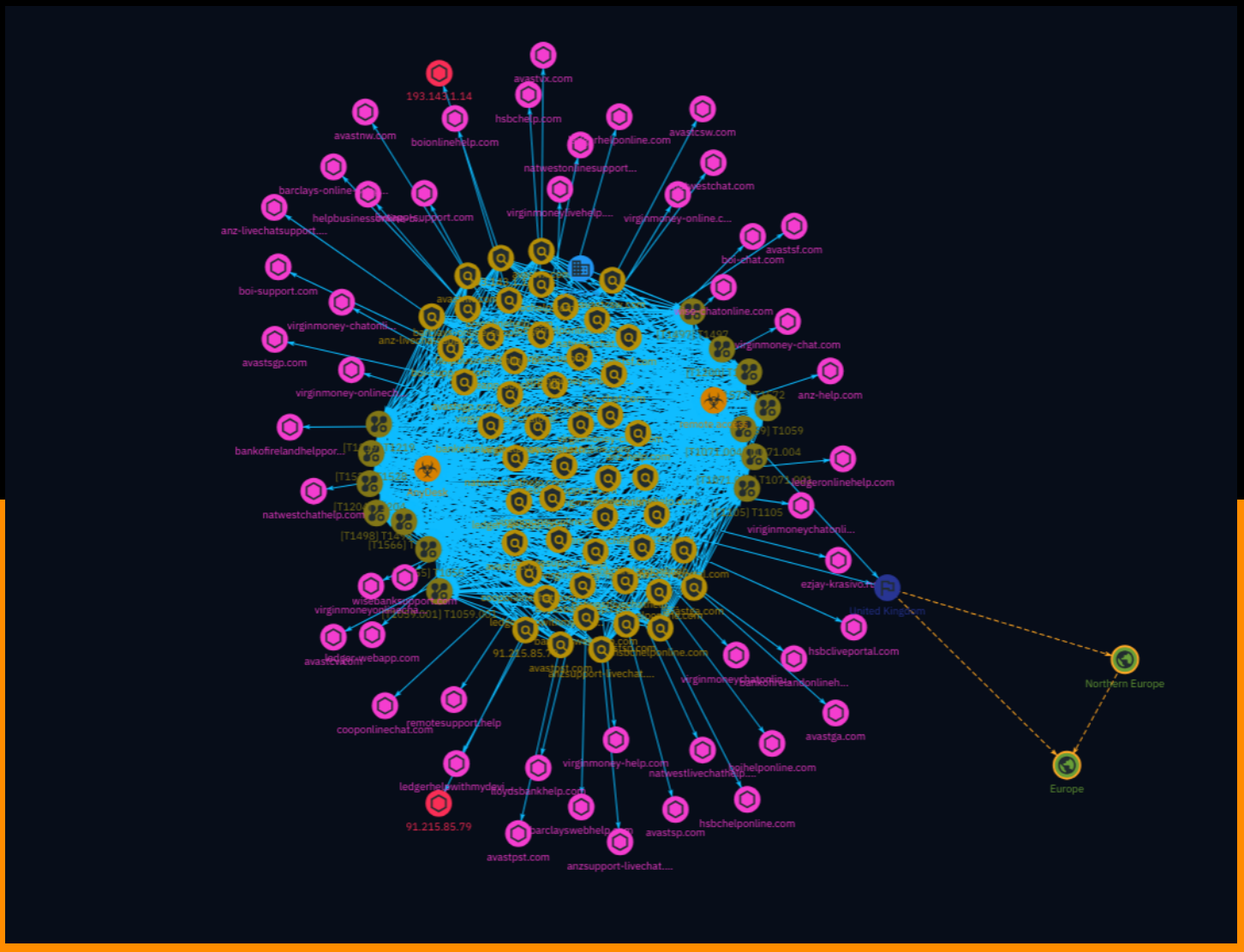

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Threat analysts are tracking an ongoing campaign that employs fake websites and social engineering tactics to distribute a malicious version of the AnyDesk remote access software to Windows and macOS users. Once installed on a victim's machine, it is being utilized to steal data and money. The campaign primarily targets UK banks like HSBC, Natwest, Lloyds, Santander, and Virgin Money, as well as Avast, Ledger, and Wise.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Attack-Pattern

Name

T1497

ID

T1497

Description

Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) during automated discovery to shape follow-on behaviors.(Citation: Deloitte Environment Awareness) Adversaries may use several methods to accomplish [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) such as checking for security monitoring tools (e.g., Sysinternals, Wireshark, etc.) or other system artifacts associated with analysis or virtualization. Adversaries may also check for legitimate user activity to help determine if it is in an analysis environment. Additional methods include use of sleep timers or loops within malware code to avoid operating within a temporary sandbox. (Citation: Unit 42 Pirpi July 2015)

Name

T1498

ID

T1498

Description

Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth services rely on. Example resources include specific websites, email services, DNS, and web-based applications. Adversaries have been observed conducting network DoS attacks for political purposes(Citation: FireEye OpPoisonedHandover February 2016) and to support other malicious activities, including distraction(Citation: FSISAC FraudNetDoS September 2012), hacktivism, and extortion. (Citation: Symantec DDoS October 2014) A Network DoS will occur when the bandwidth capacity of the network connection to a system is exhausted due to the volume of malicious traffic directed at the resource or the network connections and network devices the resource relies on. For example, an adversary may send 10Gbps of traffic to a server that is hosted by a network with a 1Gbps connection to the internet. This traffic can be generated by a single system or multiple systems spread across the internet, which is commonly referred to as a distributed DoS (DDoS). To perform Network DoS attacks several aspects apply to multiple methods, including IP address spoofing, and botnets.
Adversaries may use the original IP address of an attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking system or to enable reflection. This can increase the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the source address on network defense devices. For DoS attacks targeting the hosting system directly, see [Endpoint Denial of Service](https://attack.mitre.org/techniques/T1499).

Name

T1528

ID

T1528

Description

Adversaries can steal application access tokens as a means of acquiring credentials to access remote systems and resources. Application access tokens are used to make authorized API requests on behalf of a user or service and are commonly used as a way to access resources in cloud and container-based applications and software-as-a-service (SaaS).(Citation: Auth0 - Why You Should Always Use Access Tokens to Secure APIs Sept 2019) Adversaries who steal account API tokens in cloud and containerized environments may be able to access data and perform actions with the permissions of these accounts, which can lead to privilege escalation and further compromise of the environment. For example, in Kubernetes environments, processes running inside a container may communicate with the Kubernetes API server using service account tokens. If a container is compromised, an adversary may be able to steal the container's token and thereby gain access to Kubernetes API commands.(Citation: Kubernetes Service Accounts) Similarly, instances within continuous-development / continuous-integration (CI/CD) pipelines will often use API tokens to authenticate to other services for testing and deployment. (Citation: Cider Security Top 10 CICD Security Risks) If these pipelines are compromised, adversaries may be able to steal these tokens and leverage their privileges. Token theft can also occur through social engineering, in which case user action may be required to grant access. OAuth is one commonly implemented framework that issues tokens to users for access to systems. An application desiring access to cloud-based services or protected APIs can gain entry using OAuth 2.0 through a variety of authorization protocols. An example commonly-used sequence is Microsoft's Authorization Code Grant flow.(Citation: Microsoft Identity Platform Protocols May 2019)(Citation: Microsoft - OAuth Code Authorization flow - June 2019) An OAuth access token enables a third-party application to interact with resources containing user data in the ways requested by the application without obtaining user credentials. Adversaries can leverage OAuth authorization by constructing a malicious application designed to be granted access to resources with the target user's OAuth token.(Citation: Amnesty OAuth Phishing Attacks, August 2019)(Citation: Trend Micro Pawn Storm OAuth 2017) The adversary will need to complete registration of their application with the authorization server, for example Microsoft Identity Platform using Azure Portal, the Visual Studio IDE, the command-line interface, PowerShell, or REST API calls.(Citation: Microsoft - Azure AD App Registration - May 2019) Then, they can send a [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002) to the target user to entice them to grant access to the application. Once the OAuth access token is granted, the application can gain potentially long-term access to features of the user account through [Application Access Token](https://attack.mitre.org/techniques/T1550/001). (Citation: Microsoft - Azure AD Identity Tokens - Aug 2019) Application access tokens may function within a limited lifetime, limiting how long an adversary can utilize the stolen token. However, in some cases, adversaries can also steal application refresh tokens(Citation: Auth0 Understanding Refresh Tokens), allowing them to obtain new access tokens without prompting the user.

Name

T1200

ID

T1200

Description

Adversaries may introduce computer accessories, networking hardware, or other computing devices into a system or network that can be used as a vector to gain access. Rather than just connecting and distributing payloads via removable storage (i.e. [Replication Through Removable Media](https://attack.mitre.org/techniques/T1091)), more robust hardware additions can be used to introduce new functionalities and/or features into a system that can then be abused. While public references of usage by threat actors are scarce, many red teams/penetration testers leverage hardware additions for initial access. Commercial and open source products can be leveraged with capabilities such as passive network tapping, network traffic modification (i.e. [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557)), keystroke injection, kernel memory reading via DMA, addition of new wireless access to an existing network, and others.(Citation: Ossmann Star Feb 2011)(Citation: Aleks Weapons Nov 2015)(Citation: Frisk DMA August 2016)(Citation: McMillan Pwn March 2012)

Name

T1055

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There

are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Name

T1566

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

T1071.001

ID

T1071.001

Description

Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Protocols such as HTTP/S(Citation: CrowdStrike Putter Panda) and WebSocket(Citation: Brazking-Websockets) that carry web traffic may be very common in environments. HTTP/S packets have many fields and headers in which data can be concealed. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.

Name

T1059.001

ID

T1059.001

Description

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems). PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk. A number of PowerShell-based offensive testing tools are available, including [Empire](https://

attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack) PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying `System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)

Name

T1204

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary; running malicious JavaScript in their browser, allowing adversaries to [Steal Web Session Cookie](https://attack.mitre.org/techniques/T1539)s; or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204).(Citation: Talos Roblox Scam 2023)(Citation: Krebs Discord Bookmarks 2023) For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

T1572

ID

T1572

Description

Adversaries may tunnel network communications to and from a victim system within a separate protocol to avoid detection/network filtering and/or enable access to otherwise unreachable systems. Tunneling involves explicitly encapsulating a protocol within another. This behavior may conceal malicious traffic by blending in with existing traffic and/or provide an outer layer of encryption (similar to a VPN). Tunneling could also enable routing of network packets that would otherwise not reach their intended destination, such as SMB, RDP, or other traffic that would be filtered by network appliances or not routed over the Internet. There are various means to encapsulate a protocol within another protocol. For example, adversaries may perform SSH tunneling (also known as SSH port forwarding), which involves forwarding arbitrary data over an encrypted SSH tunnel. (Citation: SSH Tunneling) [Protocol Tunneling](https://attack.mitre.org/techniques/T1572) may also be abused by adversaries during [Dynamic Resolution](https://attack.mitre.org/techniques/T1568). Known as DNS over HTTPS (DoH), queries to resolve C2 infrastructure may be encapsulated within encrypted HTTPS packets.(Citation: BleepingComp Godlua JUL19) Adversaries may also leverage [Protocol Tunneling](https://attack.mitre.org/techniques/T1572) in conjunction with [Proxy](https://attack.mitre.org/techniques/T1090) and/or [Protocol Impersonation](https://attack.mitre.org/techniques/T1001/003) to further conceal C2 communications and infrastructure.

Name

T1105

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`. (Citation: t1105_lolbas) Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Adversaries have also abused file application features, such as the Windows `search-ms` protocol handler, to deliver malicious files to victims through remote file searches invoked by [User Execution](https://attack.mitre.org/techniques/T1204) (typically after interacting with [Phishing](https://attack.mitre.org/techniques/T1566) lures).(Citation: T1105: Trellix_search-ms) Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.(Citation: Dropbox Malware Sync)

Name

T1219

ID

T1219

Description

An adversary may use legitimate desktop support and remote access software to establish an interactive command and control channel to target systems within networks. These services, such as `VNC`, `Team Viewer`, `AnyDesk`, `ScreenConnect`, `LogMein`, `AmmyyAdmin`, and other remote monitoring and management (RMM) tools, are commonly used as legitimate technical support software and may be allowed by

application control within a target environment.(Citation: Symantec Living off the Land) (Citation: CrowdStrike 2015 Global Threat Report)(Citation: CrySyS Blog TeamSpy) Remote access software may be installed and used post-compromise as an alternate communications channel for redundant access or as a way to establish an interactive remote desktop session with the target system. They may also be used as a component of malware to establish a reverse connection or back-connect to a service or adversary-controlled system. Adversaries may similarly abuse response features included in EDR and other defensive tools that enable remote access. Installation of many remote access software may also include persistence (e.g., the software's installation routine creates a [Windows Service](https://attack.mitre.org/techniques/T1543/003)). Remote access modules/features may also exist as part of otherwise existing software (e.g., Google Chrome's Remote Desktop).(Citation: Google Chrome Remote Desktop)(Citation: Chrome Remote Desktop)

Name

T1059

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution.

(Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

T1071.004

ID

T1071.004

Description

Adversaries may communicate using the Domain Name System (DNS) application layer protocol to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. The DNS protocol serves an administrative function in computer networking and thus may be very common in environments. DNS traffic may also be allowed even before network authentication is completed. DNS packets contain many fields and headers in which data can be concealed. Often known as DNS tunneling, adversaries may abuse DNS to communicate with systems under their control within a victim network while also mimicking normal, expected traffic. (Citation: PAN DNS Tunneling)(Citation: Medium DnsTunneling)

Sector

Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.

Indicator

Name
virginmoneylivehelp.com
Pattern Type
stix
Pattern
[domain-name:value = 'virginmoneylivehelp.com']
Name
helpbusinessonline-boi.com
Pattern Type
stix
Pattern
[domain-name:value = 'helpbusinessonline-boi.com']
Name
ledgerhelpwithmydevice.com

Pattern Type
stix
Pattern
[domain-name:value = 'ledgerhelpwithmydevice.com']
Name
natwestonlinesupport.com
Pattern Type
stix
Pattern
[domain-name:value = 'natwestonlinesupport.com']
Name
ledgerhelponline.com
Pattern Type
stix
Pattern
[domain-name:value = 'ledgerhelponline.com']
Name
boionlinehelp.com

Pattern Type
stix
Pattern
[domain-name:value = 'boionlinehelp.com']
Name
avastnw.com
Pattern Type
stix
Pattern
[domain-name:value = 'avastnw.com']
Name
remotesupport.help
Pattern Type
stix
Pattern
[domain-name:value = 'remotesupport.help']
Name
anz-help.com

Pattern Type
stix
Pattern
[domain-name:value = 'anz-help.com']
Name
boihelponline.com
Pattern Type
stix
Pattern
[domain-name:value = 'boihelponline.com']
Name
anzsupport-livechat.com
Pattern Type
stix
Pattern
[domain-name:value = 'anzsupport-livechat.com']
Name
avastsgp.com

Pattern Type
stix
Pattern
[domain-name:value = 'avastsgp.com']
Name
virginmoney-online.com
Pattern Type
stix
Pattern
[domain-name:value = 'virginmoney-online.com']
Name
virginmoney-chatonline.com
Pattern Type
stix
Pattern
[domain-name:value = 'virginmoney-chatonline.com']
Name
ledger-webapp.com

Pattern Type
stix
Pattern
[domain-name:value = 'ledger-webapp.com']
Name
avastsf.com
Pattern Type
stix
Pattern
[domain-name:value = 'avastsf.com']
Name
hsbchelp.com
Pattern Type
stix
Pattern
[domain-name:value = 'hsbchelp.com']
Name
wisebanksupport.com

Pattern Type
stix
Pattern
[domain-name:value = 'wisebanksupport.com']
Name
virginmoney-onlinechat.com
Pattern Type
stix
Pattern
[domain-name:value = 'virginmoney-onlinechat.com']
Name
boi-support.com
Pattern Type
stix
Pattern
[domain-name:value = 'boi-support.com']
Name
liveapp-support.com

Pattern Type
stix
Pattern
[domain-name:value = 'liveapp-support.com']
Name
avastvx.com
Pattern Type
stix
Pattern
[domain-name:value = 'avastvx.com']
Name
bankofirelandhelpportal.com
Pattern Type
stix
Pattern
[domain-name:value = 'bankofirelandhelpportal.com']
Name
avastcsw.com

Pattern Type
stix
Pattern
[domain-name:value = 'avastcsw.com']
Name
virginmoneychatonline.com
Pattern Type
stix
Pattern
[domain-name:value = 'virginmoneychatonline.com']
Name
natwestlivechathelp.com
Pattern Type
stix
Pattern
[domain-name:value = 'natwestlivechathelp.com']
Name
barclays-online-support.com

Pattern Type
stix
Pattern
[domain-name:value = 'barclays-online-support.com']
Name
virginmoneyonlinechat.com
Pattern Type
stix
Pattern
[domain-name:value = 'virginmoneyonlinechat.com']
Name
avastpst.com
Pattern Type
stix
Pattern
[domain-name:value = 'avastpst.com']
Name
bankofirelandonlinehelp.com

Pattern Type

stix

Pattern

[domain-name:value = 'bankofirelandonlinehelp.com']

Name

91.215.85.79

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.215.85.79']

Name

virginmoney-help.com

Pattern Type

stix

Pattern

[domain-name:value = 'virginmoney-help.com']

Name

ezjay-krasivo.ru

Pattern Type
stix
Pattern
[domain-name:value = 'ezjay-krasivo.ru']
Name
hsbcliveportal.com
Pattern Type
stix
Pattern
[domain-name:value = 'hsbcliveportal.com']
Name
viriginmoneychatonline.com
Pattern Type
stix
Pattern
[domain-name:value = 'viriginmoneychatonline.com']
Name
boi-chat.com

Pattern Type
stix
Pattern
[domain-name:value = 'boi-chat.com']
Name
avastsp.com
Pattern Type
stix
Pattern
[domain-name:value = 'avastsp.com']

Domain-Name

Value
remotesupport.help
cooponlinechat.com
anzsupport-livechat.com
ledgeronlinehelp.com
avastsgp.com
avastvx.com
virginmoney-help.com
virginmoneychatonline.com
ledger-webapp.com
anz-livechatsupport.com
virginmoneylivehelp.com
wisebanksupport.com
avastsp.com

boi-chat.com

helpbusinessonline-boi.com

avastsf.com

hsbcliveportal.com

hsbchelp.com

ledgerhelpwithmydevice.com

avastga.com

natwestchathelp.com

virginmoney-online.com

virginmoney-chatonline.com

liveapp-support.com

natwestchat.com

natwestonlinesupport.com

barclays-online-support.com

barclayswebhelp.com

virginmoney-onlinechat.com

boihelponline.com

ledgerhelponline.com

wise-chatonline.com

bankofirelandhelpportal.com

boionlinehelp.com

lloydsbankhelp.com

avastpst.com

virginmoneyonlinechat.com

boi-support.com

ezjay-krasivo.ru

virginmoney-chat.com

viriginmoneychatonline.com

natwestlivechathelp.com

avastcv.com

hsbchelponline.com

avastcsw.com

avastnw.com

bankofirelandonlinehelp.com

anz-help.com

External References

- https://www.silentpush.com/blog/anydesk/
- https://otx.alienvault.com/pulse/66b6015a88b2c3482d93c9f1