TIR-20250827 Threat Actors Abusing Microsoft Quick Assist for Ransomware and Remote Access Campaigns

8/27/2025

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

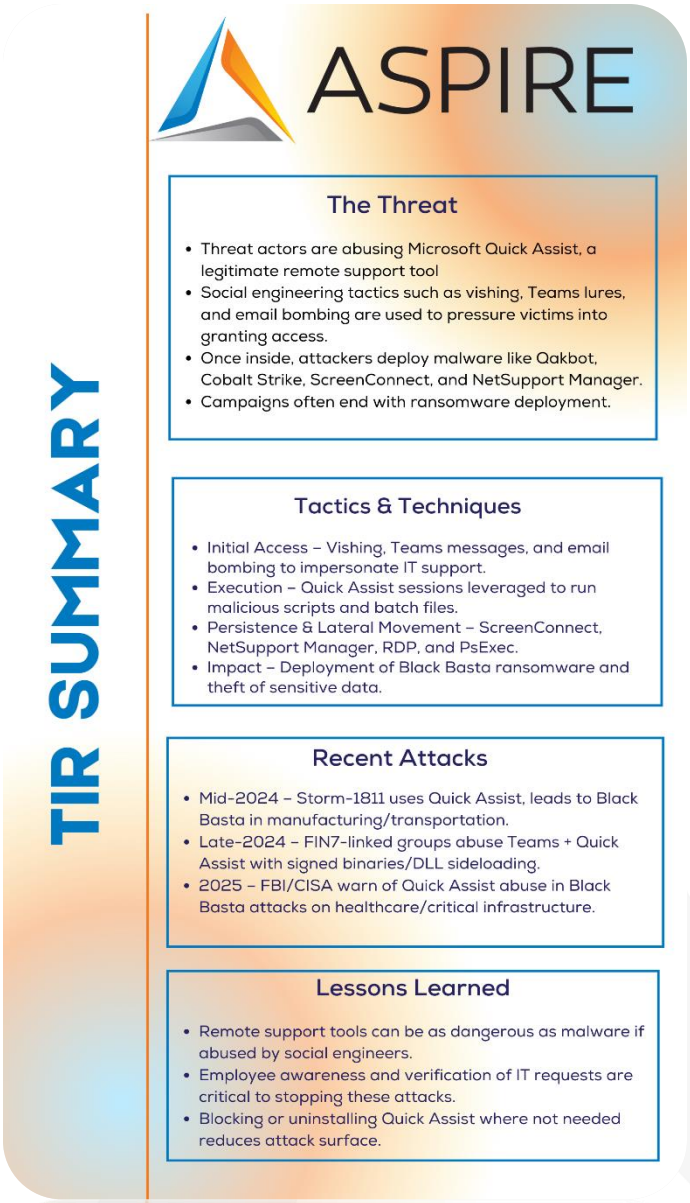
Executive Summary 3
What is Quick Assist? 4
Quick Assist Abuse 5
Threat Actors Abusing Quick Assist 6
Recent Attacks 9
Aspire Case Study 10
Conclusion 12
Aspire's Recommendations 12
MITRE MAP 13
Aspire Protects 14
Indicators of Compromise (IoCs) 15
Supporting Documentation 20
Appendix II: Disclaimer 22

Executive Summary

Since mid-2024, threat actors have increasingly abused Microsoft's built-in remote

support application, Quick Assist, to gain initial access into corporate environments. What began as a trusted IT troubleshooting tool has now become a favored pathway for social engineering campaigns. Threat actors impersonate help desk staff or IT support, convince victims to grant access, and use that foothold to deliver malware and, eventually, ransomware.

This report provides an in-depth look at how Quick Assist is being misused, with a focus on three major groups: Storm-1811, FIN7, and Black Basta affiliates. Each has leveraged Quick Assist in distinct ways, but their goals are the same. They all establish remote access and deploy ransomware to pressure organizations into paying. The campaigns often combine vishing, email bombing, or Teams-based social engineering with Quick Assist, followed by the delivery of malware families such as Qakbot, Cobalt Strike, and custom RATs.



This report discusses how Quick Assist abuse evolved and what it means for organizations across sectors. Research shows the technical side of these attacks isn't complicated, it's the social engineering that works. That's why the real defenses here are user awareness and tighter controls around remote access tools.

Quick Assist abuse isn't going away. It's becoming part of the playbook for multiple ransomware groups. As long as remote support tools stay wide open and users aren't trained to spot the tricks, attackers will keep using them. Defenders need to go beyond patching and rethink their trust in software that comes pre-installed and looks legitimate.

What is Quick Assist?

Quick Assist is a remote support tool developed by Microsoft. It allows one user (the "helper") to connect to another person's Windows device and either view their screen or take full control. The purpose is legitimate, and IT staff, teachers, or family members can use it to troubleshoot issues remotely without requiring third-party software. A six-digit code generated within Quick Assist authorizes the connection, and the recipient must consent to share their screen or hand over control.

Because Quick Assist is installed by default on Windows 11 and widely available in Windows 10 through the Microsoft Store, it has become an attractive tool for attackers. It requires no separate download, is digitally signed by Microsoft, and typically runs with user trust. These features mean it blends into normal environments far more easily than malware-flagged remote administration tools.

Quick Assist is not necessarily insecure. However, as with other living-off-the-land (LOTL) tools, attackers exploit the trust built into its brand and functionality. This makes it an ideal vehicle for social engineering. A user is far more likely to comply with an IT technician asking them to press *CTRL* + *Windows* + *Q* and enter a code than they are to install an unknown executable.

Another reason Quick Assist is frequently misused is that it does not require elevated technical knowledge. An attacker only needs a convincing script, a phone number, and a cooperative victim to establish access. Once inside, they can layer more advanced tools or payloads. That simplicity is why Quick Assist has become a recurring feature of ransomware attacks across several groups.

Quick Assist Abuse

The earliest widespread reports of Quick Assist abuse surfaced in April 2024, when Microsoft publicly documented Storm-1811's campaigns. These operations relied heavily on voice phishing calls, with actors impersonating IT staff to persuade users to initiate Quick Assist sessions. Once connected, they dropped payloads like Qakbot and Cobalt Strike, paving the way for Black Basta ransomware deployment.

By May 2024, security vendors and incident response firms observed a sharp increase in Quick Assist–based intrusions. A common precursor tactic was email bombing. Attackers would sign victims' email addresses up for thousands of newsletters, flooding their inboxes. They then called the victims, pretended to be IT support offering to "fix the spam problem," and used Quick Assist to gain access. This pairing of fake urgency and a legitimate Microsoft tool created a high success rate for social engineering.

Other campaigns evolved by June 2024 to incorporate Microsoft Teams messages and calls. Threat actors used external tenants with names like "Help Desk IT" or "Microsoft Security" to appear legitimate. Victims who trusted these calls often granted Quick Assist access, which was then abused to install ScreenConnect, NetSupport Manager, and SystemBC RAT.

Key techniques documented across these campaigns include:

- Vishing and impersonation of IT/help desk personnel
- Abuse of Quick Assist codes to establish trusted remote access
- Ingress tool transfer using cURL and BITS jobs for batch files and ZIP payloads
- Credential theft via EvilProxy and browser data access
- Follow-on tools like ScreenConnect, NetSupport Manager, and Cobalt Strike

The abuse of Quick Assist has since been picked up by other groups beyond Storm-1811. Affiliates of Black Basta and operators linked to FIN7 have adopted similar approaches, showing how quickly effective techniques spread across the cybercrime ecosystem. Unlike vulnerabilities, these attacks don't depend on unpatched software, they depend on users being tricked into granting access, making it harder to defend against with technical controls alone.

Over time, Quick Assist has become more than just a one-off trick; it is now a recognized step in the ransomware lifecycle. It lowers the barrier to entry for attackers while simultaneously neutralizing the user's instinct to be suspicious. If the request comes through a familiar Microsoft-branded tool, many people assume it's safe.

Threat Actors Abusing Quick Assist

Storm-1811

Storm-1811 is a financially motivated threat actor first documented by Microsoft in April 2024. Known for deploying Black Basta ransomware, it has specialized in voice phishing and Quick Assist exploitation to establish initial access. Microsoft and other vendors have tied them to a pattern of tech support scams where they impersonate IT staff and abuse Quick Assist sessions to install malware.

- **Country of Origin** - Believed to operate from Russia or Russian-speaking regions.
- **Aliases** - Sometimes referred to in vendor reporting as part of the Black Basta affiliate network.
- **TTPs** - Vishing, Quick Assist sessions, Teams phishing, email bombing, Qakbot delivery, Cobalt Strike, PsExec for lateral movement, Black Basta ransomware deployment.
- **Industries Impacted** - Manufacturing, construction, food and beverage, transportation, healthcare, and professional services.
- **First Observed** - April 2024 (Microsoft reporting).
- **Connections** - Works directly with Black Basta operators; overlaps with other ransomware-as-a-service initial access brokers.
- **Operations Status** - Ongoing; no confirmed arrests or shutdowns.
- **Motivation** - Financial, using double-extortion ransomware.

- **Ransom Demands/Payments** - Black Basta demands range from hundreds of thousands to millions; affiliates like Storm-1811 receive a cut.

Storm-1811 stands out because it doesn't just hand off access. In several cases, the group stayed active in environments post-ransomware deployment, monitoring for recovery attempts. This behavior means that the threat actor plays a dual role. They are both initial access brokers and active affiliate, a rare but increasingly common trait among modern ransomware groups.

FIN7

FIN7, also known as Carbanak or Sangria Tempest, is one of the most notorious financially motivated threat groups, active since at least 2013. While originally tied to point-of-sale malware and large-scale financial theft, in recent years FIN7 has shifted toward ransomware collaboration and remote access intrusions. Reporting in 2024 and 2025 shows FIN7 or clusters strongly linked to it leveraging Quick Assist, Teams messages, and DLL sideloading for access and persistence.

- **Country of Origin** - Primarily Russian-speaking cybercriminal ecosystem.
- **Aliases** - Carbanak, Sangria Tempest.
- **TTPs** - Quick Assist misuse, Teams phishing, DLL sideloading via signed binaries (TeamViewer.exe), PowerShell for payload delivery, BITS jobs, credential theft from browsers, PsExec for lateral movement.
- **Industries Impacted** - Retail, finance, hospitality, manufacturing, healthcare.
- **First Observed** - 2013 (Carbanak banking trojan); Quick Assist campaigns documented in 2024/2025.
- **Connections** - Linked to Black Basta and BlackSuit through shared tooling, infrastructure, and malware (Anubis RAT).
- **Operations Status** - Despite multiple arrests of FIN7 members in the past, the group remains active in various forms.
- **Motivation** - Financial; tied to ransomware ecosystems and direct theft.

- **Ransom Demands/Payments** - Past ransomware collaborations demanded millions; cumulative financial theft attributed to FIN7 exceeds $1 billion historically.

What makes FIN7 a threat is its ability to adapt and masquerade. The group previously built fake cybersecurity firms, hiring real security professionals under the false belief they were doing legitimate work. That same kind of deception now extends into their Quick Assist and Teams-based social engineering campaigns, making them harder to distinguish from legitimate IT activity.

Black Basta

Black Basta is a ransomware group first observed in April 2022. Unlike RaaS models, Black Basta is believed to be a closed operation, run by a smaller set of operators and trusted affiliates. Quick Assist abuse has become a core part of its affiliates' initial access campaigns, along with ScreenConnect, NetSupport Manager, and Teams phishing.

- **Country of Origin** - Russian-speaking threat actor network.
- **Aliases** - None officially, though sometimes connected to Conti lineage.
- **TTPs** - Quick Assist vishing, Teams phishing, credential theft (EvilProxy), Qakbot and Cobalt Strike deployment, PsExec for ransomware distribution, RClone for exfiltration, Backstab tool to disable EDR.
- **Industries Impacted** - At least 12 of 16 U.S. critical infrastructure sectors, including healthcare, energy, and manufacturing. Over 500 organizations impacted worldwide by May 2024.
- **First Observed** - April 2022.
- **Connections** - Works with Storm-1811 for access; overlaps with FIN7 in tooling.
- **Operations Status** - Active and expanding; no arrests reported.
- **Motivation** - Financial, double-extortion ransomware.
- **Ransom Demands/Payments** - Demands typically range from $500K to $2M+; exact payments not always disclosed but estimated in the tens of millions.

One distinctive trait of Black Basta is its discipline compared to other ransomware groups. They operate with consistency, using repeatable toolchains like Quick Assist, Qakbot, and PsExec, which allows defenders to map and anticipate their behavior. Their success shows that even modest innovations, like swapping phishing emails for Teams calls, can pay off when layered on top of reliable ransomware infrastructure.

Recent Attacks

April 2024 – Storm-1811 Campaign

Microsoft observed Storm-1811 beginning widespread Quick Assist abuse, using vishing to impersonate IT support. Victims were convinced to launch Quick Assist and provide access codes, leading to Qakbot and Cobalt Strike deployment. The campaign culminated in Black Basta ransomware across multiple industries. Attackers also carried out inbox flooding to reinforce the sense of urgency, showing how multiple social engineering levers can be combined for greater effect.

May 2024 – Email Bomb and Quick Assist Abuse

Rapid7 and others reported that Black Basta affiliates combined massive email floods with phone calls impersonating IT staff. The spam created urgency, and Quick Assist was the proposed “fix.” Once remote access was granted, PsExec was used to spread ransomware laterally. In several cases, manufacturing firms suffered production outages lasting days, proving that even simple initial access techniques can have heavy operational impacts.

June 2024 – Microsoft Teams Phishing

Microsoft documented Black Basta affiliates using Teams to message targets as “Help Desk IT.” Victims tricked into Quick Assist sessions later faced credential theft through EvilProxy and persistence via SystemBC RAT. This evolution was a key shift because attackers no longer relied solely on cold calls but used trusted enterprise platforms to reinforce their impersonation, which increases the success rate of initial access.

January 2025 – Sophos Cases

Sophos MDR reported at least 15 incidents of email bombing followed by Teams vishing and Quick Assist abuse between November 2024 and January 2025. Two tracked clusters (STAC5143 and STAC5777) showed overlaps with FIN7 and Storm-1811, confirming that Quick Assist abuse has spread beyond a single group. These investigations revealed that Quick Assist is now an ecosystem-wide technique, not just the tool of one actor.

Aspire Case Study

In a case researched by Aspire's Digital Forensics lead and SOC Analysts, a customer received a phone call directly from a malicious actor impersonating IT support. The caller attempted to convince the user to open Quick Assist and provide a session code. The goal was to gain remote access under the guise of "fixing a technical issue".

The attacker's social engineering mirrored the patterns seen in Storm-1811 and Black Basta campaigns, particularly impersonation of IT staff and phone-based vishing. However, unlike documented incidents where Quick Assist sessions were successfully established, this attempt was interrupted before further malware delivery could occur.

Key TTPs observed included impersonation (T1656 - Impersonation) and attempted Quick Assist misuse (T1219 – Remote Access Tools). The attacker's reliance on direct voice phishing shows an overlap with Storm-1811 tactics. No evidence was seen of Qakbot, Cobalt Strike, or ransomware in this case, which means it may have been an early-stage attempt or a less resourced/experienced operator.

Comparing this incident to other campaigns, the attack vector is identical. The only difference is that in this case, the intrusion was stopped at the social engineering stage. This proves why early user awareness is important. Had the Quick Assist code been shared, follow-on malware delivery and eventual ransomware deployment would have been possible.

This case also demonstrates that Quick Assist abuse does not always require heavy infrastructure or coordination. A single actor with a convincing phone script can launch an attack attempt. While that doesn't guarantee success, it reinforces why defenders should prepare for low-cost, high-impact techniques that can be attempted.

SPOTTING THE SIGNS OF VISHING

Vishing is a form of social engineering where attackers use phone calls or voice messages to trick people into giving up information or granting access they normally wouldn't. The campaigns are designed to sound convincing, often with the caller pretending to be from IT support, Microsoft, or even the victim's own help desk.

Attackers typically create a sense of urgency, claiming there's an issue with email delivery, a suspicious login attempt, or a system update that must be applied right away. The voice on the other end will push the victim to act quickly, discouraging them from verifying the request through normal channels. In some cases, the call may come shortly after an email bombing attack, with the threat actor offering to "fix" the flood of messages by walking the user through remote access steps.

The key to spotting vishing is recognizing when the request feels unusual, forced, or rushed. A legitimate IT professional won't demand credentials over the phone, pressure someone to bypass security policies, or insist on using unfamiliar tools like Quick Assist without prior notice. Any call that urges immediate compliance without standard verification, especially when combined with suspicious email activity, should be treated with caution and reported.

Red Flags in a Vishing Call

- Caller insists they are IT or Microsoft support and pressures you to act immediately.
- You're asked to install or open remote access tools like Quick Assist, ScreenConnect, or TeamViewer.
- The caller discourages you from hanging up, verifying their identity, or contacting your actual IT team.
- The timing feels suspicious, such as receiving the call right after your inbox is flooded with spam or alerts.

CONCLUSION

Quick Assist has shifted from a helpful Microsoft tool into one of the most abused initial access methods in ransomware campaigns. Groups like Storm-1811, FIN7, and Black Basta affiliates exploit its built-in trust and widespread availability to trick users into handing over control of their devices. Once access is granted, the path to full compromise is short, often resulting in ransomware and extortion.

Looking forward, we can expect continued abuse of Quick Assist and other remote support tools. Attackers adapt quickly, and as awareness of Quick Assist grows, similar trusted tools may be targeted. The lesson here is that legitimate software can become a threat vector when combined with effective social engineering. Organizations must treat remote support pathways as part of their attack surface and lock them down accordingly.

Another key lesson is that abuse of Quick Assist is a social problem, not just a technical one. The underlying software works as designed, but when trust is exploited, the outcome is the same as a zero-day. This blurs the line between patching and policy, showing that organizations must harden not only their networks but also their trust boundaries and internal culture.

ASPIRE'S RECOMMENDATIONS

Organizations can reduce risk from Quick Assist abuse by taking specific actions:

- **Remove Quick Assist if not needed** - Uninstall via PowerShell (Get-AppxPackage -Name MicrosoftCorporationII.QuickAssist | Remove-AppxPackage -AllUsers) or block its endpoint (remoteassistance.support.services.microsoft.com).
- **Restrict external communications** - Limit Microsoft Teams calls and chats from external tenants unless whitelisted.

- **Implement user awareness training** - Teach staff that IT support will never cold-call them to request Quick Assist sessions or codes.
- **Enable detection for LOTL tools** - Monitor for Quick Assist, ScreenConnect, and NetSupport Manager sessions in your environment.
- **Harden authentication** - Require phishing-resistant MFA and Conditional Access policies for remote admin accounts.
- **Limit lateral movement** - Block PsExec where not needed; monitor for BITS jobs and suspicious cURL commands.
- **Incident preparedness** - Have playbooks ready for suspected Quick Assist abuse, including immediate account lockouts and forensic review.

MITRE MAP

Storm-1811

Initial Access	T1566 – Phishing T1219 – Remote Access Software
Execution	T1059.001 - Command and Scripting Interpreter: PowerShell
Persistence	T1547 – Startup Items
Lateral Movement	T1021.002 – Remote Services: SMB/Windows Admin Shares

FIN7

Initial Access	T1656 – Impersonation
Execution	T1218 – Signed Binary Proxy Execution
Persistence	T1197 – BITS Jobs
Credential Access	T1555.003 – Credentials from Password Stores: Credentials from Web Browsers
Lateral Movement	T1021.002 – Remote Services: SMB/Windows Admin Shares
Command and Control	T1090 – Proxy

Black Basta

Initial Access	T1219 – Remote Access
Execution	T1059.001 – Command and Scripting Interpreter: PowerShell
Persistence	T1053 – Scheduled Tasks
Defense Evasion	T1562.001 – Impair Defenses: Disable or Modify Tools
Exfiltration	T1041 – Exfiltration Over C2 Channel
Impact	T1486 – Data Encrypted for Impact

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.

  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.

- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.

  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

INDICATORS OF COMPROMISE (IOCS)

Storm-1811

MD5

- 580ba62ea52551e50a6e4d1f8e49d630
- 6615ea2fa3b879d27687a7ce917e93b0
- 696dc013b2d978bc100171496148db1b
- be91cd27924b64563c4d790bb4292179
- e1bcd15824471b3afc9981fd81bfdb98
- f9a37da5c10317e9b69d2199c9e34984

SHA1

- 73bf648fa87bdd26ed2a161be7e3fbd6300eb826
- 893384de883db97c39a12899cc96afdcfb11f09c
- 8d4f19b221751297b0c3a10f105772d7286c9411
- ae366b3c9338d1f96daf4f71cc95b0ea7d573fa0
- b24904a91d9c3ce2c6e4d506ca173f98bb5f7a0a
- cd41f4f69df53e33944d053c75296c805e41380c

SHA256

- 0f9156f91c387e7781603ed716dcdc3f5342ece96e155115708b1662b0f9b4d0
- 1ad05a4a849d7ed09e2efb38f5424523651baf3326b5f95e05f6726f564ccc30
- 1cb1864314262e71de1565e198193877ef83e98823a7da81eb3d59894b5a4cfb
- 2ec12f4ee375087c921be72f3bd87e6e12a2394e8e747998676754c9e3e9798e
- 35456f84bc88854f16e316290104d71a1f350e84b479eebd6fbb2f77d36bca8a
- 59f1c5fe47c1733b84360a72e419a07315fbae895dd23c1e32f1392e67313859
- 6f31cf7a11189c683d8455180b4ee6a60781d2e3f3aadf3ecc86f578d480cfa9
- 71d50b74f81d27feefbc2bc0f631b0ed7fcdf88b1abbd6d104e66638993786f8
- 76f959205d0a0c40f3200e174db6bb030a1fde39b0a190b6188d9c10a0ca07c8
- 93058bd5fe5f046e298e1d3655274ae4c08f07a8b6876e61629ae4a0b510a2f7
- a47718693dc12f061692212a354afba8ca61590d8c25511c50cfecf73534c750
- c18e7709866f8b1a271a54407973152be1036ad3b57423101d7c3da98664d108

Domains

- greekpool[.]com
- limitedtoday[.]com
- realsepnews[.]com
- rewilivak13[.]com
- thetrailbig[.]net
- upd5[.]pro
- upd7[.]com
- upd7a[.]com
- upd9[.]com
- zziveastnews[.]com
- instance-olqdnn-relay[.]screenconnect[.]com

FIN7 *(Note: This is a sample of FIN7's IoCs. For a complete list, click here.)*

MD5

- 05d400f4734d2d68af6bb916112f5a19
- 0671bd79586ae06680cfee11753f509e
- 068d55958d46c01408ca354967b482b7
- 06a6bc8bc98213d770acffb7b28b6abb

- 09576ba9ff1933617add7f14e944387b
- 0c91401af0f77c91d7d2c2d858043cc2
- 0cb3f8d4df1f2139e45b3a276fa48f25
- 0ec6ce8d2213cc9a7b570fc22e5fce1a
- 14048ed02214ef052169460340e9a420
- 14c2ce8f3c5856c8415368930bb8c1df
- 2d39a5f8bece043c706a3ff6c1c59e9a
- 318bf7ea84487c8a63a3996e24494455
- 3a0ef7cf40cc50d47cb956fce8baa456
- 3e390f3b3ca7d3716775f832c93fb1b1
- 42cb39b338f2b1bc94f5ae483b048e30
- 5085779e68656455315ca6a46157ab88
- 51feca3c49e7b0323133e85716a28a3a
- 5fcd76bddd9b41bf5c63ec660d82f977
- 610e029cb014dcec9c079ca11020c333
- 663492a2fb33c3c4a5813b880d48f7be
- 6eaa4c8938016293d2153ccd78b473fc
- 72b343b03e9197f425e6a918a2c20a47
- 797992ab276d218d7feb2e6e8b2fd678
- 798aed4d37293ea34448cf0496cfeefa
- 99b82bdc2f4559929a3a884aebacd11c
- a5685feb1b6c54ba5149ed2f7000f491
- b0fd9705e8f83129f97f9111b03642fe
- b57d2544cb7736d533af1aa07040156b
- cdb98412665135775e908564c87d5144
- d4fe37649a9778e80ae9a5a8633d2af4
- ef9de8cc533ce1848588679e61e70b15
- f899781c5239e59fd7d11c9211c08d28
- ff25441b7631d64afefdb818cfcceec7

SHA1

- 038dc2008fbafba4e086260fffc1372d3ad8b1e2
- 03b19fd1a41d0d1b55ad653341a05071b48a49ea
- 15940747af57b5a6c2d722c37dc885f45ed665dc

- 1c55e479cd0e64bbeda79758dc2b88679382cc56
- 216ad95bec4b03957c4d451ea774ba46b18ec4f4
- 21ce24bd123c9e123dffed7aae334dfb3d40c026
- 243ed6b028aeb2c94eeafbffcad193f43b808444
- 34babd4b6e3f196cb9c1064bceaf350c81a11dca
- 381b421b49f88e035b274711d315050f83c43e22
- 3b46515807a491f366d6e695288398ddab93e53f
- 515d9e04e0699dec2aa101691d166aef4d231dde
- 597275867676bb49aac9b8381db0addc4718bc12
- 5cc8837f0f87f71c5551c009a69fa12daf3254d4
- 68c20ea201ebf82aa721f75c8884bfde6c7083d7
- 6d878962e770856cac885deeff5fd75b00a02605
- 71babd331be91acc43df85ed35f3a4e9746b59be
- 8287f3a900438185a6faa2c106cf05d4a20df1b9
- 8448f344c3e05d70506899859cf61ba47bb906f2
- 94f1cb1ca20f30f4ccbf7164d4de2a2c2effa298
- 99cfbecaebc79e723603997fb2102363319103eb
- 9d55e811553bd8a7dba352a30e5aee0a90f9a118
- 9efd1954430f98554f60a58eaf76dcabfddb7fbd
- af34b30695539f108741648a1fce012bdf81cc75
- b5fcf5d6bf770cca52d7cb1e9423fa89c50a0d27
- b6c6a400435f6121ce94694702dfec51f16c6085
- c641aa50bc40c3fd1e74ed8dc85e6b7019560389
- cdd606e1955704796dec7e581b9ce30c5fdf1757
- d002071bd7dbe9ef91a843b87a56c156837015f1
- d044e629b6c0bafa9b312ab6c7f00cbcaa37b8a0
- d21b17f6ec5196c4ce3cad44ca24856b99874793
- d42cad9e12c144c243614210b12f5042aa39c35e
- e2c98ad43b3b0325bb019e4abae20aa877824dd6
- f844e720dd766f9acf89fb92434ec6e75adce09b

SHA256

- 038dc2008fbafba4e086260fffc1372d3ad8b1e2
- 03b19fd1a41d0d1b55ad653341a05071b48a49ea
- 15940747af57b5a6c2d722c37dc885f45ed665dc
- 1c55e479cd0e64bbeda79758dc2b88679382cc56
- 216ad95bec4b03957c4d451ea774ba46b18ec4f4
- 21ce24bd123c9e123dffed7aae334dfb3d40c026
- 243ed6b028aeb2c94eeafbffcad193f43b808444
- 34babd4b6e3f196cb9c1064bceaf350c81a11dca
- 381b421b49f88e035b274711d315050f83c43e22
- 3b46515807a491f366d6e695288398ddab93e53f
- 515d9e04e0699dec2aa101691d166aef4d231dde
- 597275867676bb49aac9b8381db0addc4718bc12
- 5cc8837f0f87f71c5551c009a69fa12daf3254d4
- 68c20ea201ebf82aa721f75c8884bfde6c7083d7
- 6d878962e770856cac885deeff5fd75b00a02605
- 71babd331be91acc43df85ed35f3a4e9746b59be
- 8287f3a900438185a6faa2c106cf05d4a20df1b9
- 8448f344c3e05d70506899859cf61ba47bb906f2
- 94f1cb1ca20f30f4ccbf7164d4de2a2c2effa298
- 99cfbecaebc79e723603997fb2102363319103eb
- 9d55e811553bd8a7dba352a30e5aee0a90f9a118
- 9efd1954430f98554f60a58eaf76dcabfddb7fbd
- af34b30695539f108741648a1fce012bdf81cc75
- b5fcf5d6bf770cca52d7cb1e9423fa89c50a0d27
- b6c6a400435f6121ce94694702dfec51f16c6085
- c641aa50bc40c3fd1e74ed8dc85e6b7019560389
- cdd606e1955704796dec7e581b9ce30c5fdf1757
- d002071bd7dbe9ef91a843b87a56c156837015f1
- d044e629b6c0bafa9b312ab6c7f00cbcaa37b8a0
- d21b17f6ec5196c4ce3cad44ca24856b99874793
- d42cad9e12c144c243614210b12f5042aa39c35e
- e2c98ad43b3b0325bb019e4abae20aa877824dd6
- f844e720dd766f9acf89fb92434ec6e75adce09b

URLs

- hxxp[://]31[.]boo/73689d8a-25b
- hxxps[://]cdn40[.]click/9e4e27b7-bcfb-4298-bf8f-2cf4a6bdb3bf-9b6b40d6-3f8e-4755-9063-
- hxxps[://]cdn40[.]click/9e4e27b7-bcfb-4298-bf8f-2cf4a6bdb3bf-9b6b40d6-3f8e-4755-9063-562658ebdb95'
- hxxps[://]ib[.]systems/range[.]csv
- hxxps[://]monkeybeta[.]com/crypt/Package[.]tar[.]gpg
- hxxps[://]utr-jopass[.]com/index[.]php?utm_content=$encryptedString

Black Basta

URLs

- hxxp[://]administratorIT[.]onmicrosoft[.]com
- hxxp[://]supportbotatsupportteamits[.]onmicrosoft[.]com
- hxxp[://]ACTgroup620[.]onmicrosoft[.]com

SUPPORTING DOCUMENTATION

APT Profile: FIN7 - SOCRadar® Cyber Intelligence Inc.

GrayAlpha Unmasked: New FIN7-Linked Infrastructure, PowerNet Loader, and Fake Update Attacks

Gone But Not Forgotten: Black Basta's Enduring Legacy - LevelBlue - Open Threat Exchange

Storm-1811 Performing Social Engineering to Spread Black Basta Ransomware - LevelBlue - Open Threat Exchange

FIN7, GOLD NIAGARA, ITG14, Carbon Spider, ELBRUS, Sangria Tempest, Group G0046 | MITRE ATT&CK®

How Cyber Crime Group FIN7 Attacked and Stole Data from Hundreds of U.S. Companies — FBI

Hacker group FIN7 is selling EDR evasion tools to other cyber criminals | IBM

Carbanak and FIN7 Attack Techniques | Trend Micro (US)

IOC - New FIN7-Linked Infrastructure, PowerNet Loader, and Fake Update Attacks - LevelBlue - Open Threat Exchange

On the Hunt for FIN7: Pursuing an Enigmatic and Evasive Global Criminal Operation | Mandiant | Google Cloud Blog

FIN7: Silent Push unearths 4000+ phishing and shell domains

Office of Public Affairs | High-Level Member of Hacking Group Sentenced to Prison for Scheme that Compromised Tens of Millions of Debit and Credit Cards | United States Department of Justice

FIN7-linked threat group impersonates 7-Zip, software updates | SC Media

GrayAlpha Operation Detection: The Fin7-Affiliated Group Spreads PowerNet Loader, NetSupport RAT, and MaskBat Loader | SOC Prime

New advanced FIN7's Anubis backdoor allows to gain full system control on Windows

Russian Ransomware Groups Deploy Email Bombing and Teams Vishing - Infosecurity Magazine

Windows Quick Assist Exploited in Ransomware Attacks - Infosecurity Magazine

How a fake cybersecurity firm became a real threat - Techzine Global

Threat actors misusing Quick Assist in social engineering attacks leading to ransomware | Microsoft Security Blog

Sophos MDR tracks two ransomware campaigns using “email bombing,” Microsoft Teams “vishing” – Sophos News

Storm-1811 exploits RMM tools to drop Black Basta ransomware

Storm-1811 threat actor conducts Vishing attack via Quick Assist tool

Two ransomware groups abuse Microsoft’s Office 365 platform to gain access to target organizations

Signed. Sideloaded. Compromised! | Ontinue

Solve PC problems remotely using Quick Assist - Microsoft Support

Using Quick Assist for Remote Support - Information Technology - UConn Knowledge Base

BlackSuit Escalates Social Engineering Attacks Amid Black Pasta Rift | Rapid7 Blog

#StopRansomware: Black Basta | CISA

Cybercriminals Exploiting Microsoft's Quick Assist Feature in Ransomware Attacks

Black Basta Ransomware Group Affiliates Leveraging Windows Quick Assist for Initial Access - Arctic Wolf

Black Basta ransomware affiliates use Quick Assist to target users

#StopRansomware: Black Basta

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.