TLP: AMBER For Dragos Customers

THREAT INTELLIGENCE SUMMARY

TR-2023-14: Black Basta Threatens Impact to Multiple Industries

24 May 2023

ICS Impact

On 11 May 2023, open-source media and private sources reported that the ransomware group Black Basta compromised the large Switzerland-based industrial conglomerate ABB. Dragos learned that Black Basta possibly compromised one ABB industrial partner through a trusted connection, but the connection was able to mitigate the intrusion and subsequently limited the impact. There are no further reports of adversary lateral movement after 7 May 2023, which was approximately when ABB employees reportedly viewed a Black Basta ransom note.

While Dragos is unaware if Black Basta compromised or attempted to compromise the operational technology (OT) and industrial control system (ICS) networks related to ABB, Black Basta has consistently conducted disruptive attacks across multiple industries and, therefore, represents a capable and present threat to industrial organizations in Europe and North America. Left unmitigated, Black Basta can potentially disrupt ICS, OT, and IT networks critical to operations. Dragos assesses with moderate confidence that the adversaries behind the Black Basta ransomware group will continue to impact the operations of medium and large industrial organizations through 2023.

TLP CLEAR
Approved for public release

Threat Analysis	Analyst Assessment
Audience	Information Technology (IT) / Operational Technology (OT) Security professionals and managers
Targeted Sector/Industry	All
Targeted Region	Western Europe, North America
Threat Group	N/A
Threat Intelligence Score	A far-reaching threat or vulnerability calling for action broadly across at least one industry
ICS Cyber Kill Chain Stage	Stage 1: Delivery, Exploit, Install/Modify, C2, Act
MITRE ATT&CK Techniques	Refer to Appendix
How to Confirm Compromise	C2 communication or exfiltration to hosts using self-signed certificates, anomalously large outbound data flow

Best Course of Action	Employ critical ICS controls. Hunt for, detect, and mitigate against known Black Basta TTPs, especially the five Black Basta tactics outlined in this advisory.
IOC Availability	Yes

TLP CLEAR
Approved for public release

TR-2023-14: Black Basta Threatens Impacts to Multiple Industries

24 May 2023

TLP: AMBER FOR DRAGOS CUSTOMERS ONLY

● A limited threat, risk, or vulnerability requires an applicability assessment before taking action.

THIS INFORMATION IS PROVIDED "AS-IS" AND FOR INFORMATIONAL PURPOSES ONLY, WITH NO WARRANTY EXPRESS OR IMPLIED. YOU (AND ANY PERSON OR ENTITY WHO YOU ARE ACTING ON BEHALF OF) ARE SOLELY RESPONSIBLE FOR ALL ACTS AND OMISSIONS TAKEN IN RELIANCE ON THIS INFORMATION, AND DRAGOS WILL NOT HAVE ANY RESPONSIBILITY OR LIABILITY FOR ANY SUCH ACTS OR OMISSIONS.

For definitions of confidence levels in Dragos assessments and Traffic Light Protocols for sharing, see the FAQ section in the WorldView Portal. Questions? Submit a support request through the WorldView Portal.

TLP CLEAR
Approved for public release

Executive Summary

On 11 May 2023, open-source media and private sources reported that the ransomware group Black Basta compromised the large Switzerland-based industrial conglomerate ABB. ABB provides industrial automation and process control equipment and services across various industries worldwide, including energy (electric, nuclear, renewable, oil and natural gas (ONG)), utilities, marine, rail, automotive, transport, and manufacturing. Dragos learned that on or before 7 May 2023, ABB employees were presented with Black Basta's ransom note demanding a significant monetary sum. Dragos learned that Black Basta possibly compromised one ABB industrial partner through a trusted connection, but the connection was able to mitigate the intrusion and subsequently limited the impact.

There are no further reports of adversary-lateral movement after 7 May 2023. However, shift workers at a Hitachi Energy manufacturing plant in the U.S. state of Missouri reported plant disruptions to a Jefferson City, Missouri, television station. Subsequently, Hitachi Energy confirmed with the television station that it had halted manufacturing operations and canceled shifts on 8 May 2023 "due to ongoing network disruptions of one of our service providers." While Dragos can confirm that Hitachi Energy has an operations and services relationship with ABB, at this time, Dragos cannot confirm if the Hitachi Energy operations disruptions are directly related to the Black Basta attack on ABB.

While Dragos has received no direct information from ABB, Dragos confirmed that trusted network connections were proactively and broadly severed between ABB and multiple ABB customers and partner organizations. Private reports indicate that the direct impact on ABB from the ransomware adversary activity may be limited to only specific ABB business units and facilities. Dragos is unaware if Black Basta compromised or attempted to compromise OT and ICS networks related to ABB.

Since October 2022, Black Basta double-extortion ransomware attacks have caused significant operational disruption to large industrial targets, including AGCO[1] (agricultural machinery manufacturing), Aurubis AG (metals and mining), Dole Food (food and beverage), and Kenworth (automotive manufacturing) through the intrusion on Kenworth's manufacturing partner, Riffle Machine Works. Black Basta thus represents a capable and present threat to industrial organizations in Europe and North America.

Dragos is publishing this threat report to help inform network owners supporting critical operations about the most efficient defense and detection and mitigation against targeted Black Basta attacks. Network defenders should know that Black Basta has successfully evaded Endpoint Detection and Response (EDR) regimes and established administrative privileges on large target networks. Network owners need robust visibility with multiple layered controls (defense-in-depth) to defend against this threat successfully. The Black Basta tactics to focus your detection, mitigation, and hunting efforts include malware delivery through email thread hijacking, self-signed Transport Layer Security (TLS) certificates for command and control (C2) and exfiltration, C2 over Domain Name System (DNS) protocol, and anomalous outbound data flow. Left unmitigated, Black Basta can potentially disrupt the ICS, OT, and IT networks critical to operations. Dragos recommends reviewing the included IOCs and augmenting the defenses against Black Basta tactics that are outlined in this report.

Key Findings

- The Black Basta ransomware group compromised ABB networks on or before 7 May 2023 with reports of a ransom note demanding a significant monetary sum.
- The Black Basta ransomware attack on ABB highlights a capable threat against multiple industries worldwide.
- Black Basta has demonstrated the ability to disrupt operations in multiple sectors.
- Defenders of critical operation network owners should review and act on the included IOCs and augment defenses against the Black Basta tactics outlined in this report.

Contents

[1] AGCO Ransomware Incident – Dragos WorldView

TLP CLEAR
Approved for public release

TLP CLEAR
Approved for public release

Countering Black Basta

Black Basta is a Russian-speaking, highly capable, double-extortion ransomware group that has been active since April 2022. Double extortion means the adversary steals data and exfiltrates it from the targeted network before encrypting the computers and systems. The adversary then threatens to leak the stolen data to pressure the target into paying the ransom. Multiple researchers have noted links between Black Basta and the notorious since-dissolved ransomware groups Conti and REvil[2]. Black Basta compromised ABB networks and, according to private reports, possibly exfiltrated a significant amount of data sometime before 7 May 2023, when the first reports emerged of a Black Basta ransom note with substantial monetary demand. Dragos is currently unaware of the initial intrusion vector into ABB's targeted network or network. However, Dragos assesses with moderate confidence that defending against the following five Black Basta tactics can boost defensive postures while minimizing additional cybersecurity resources.

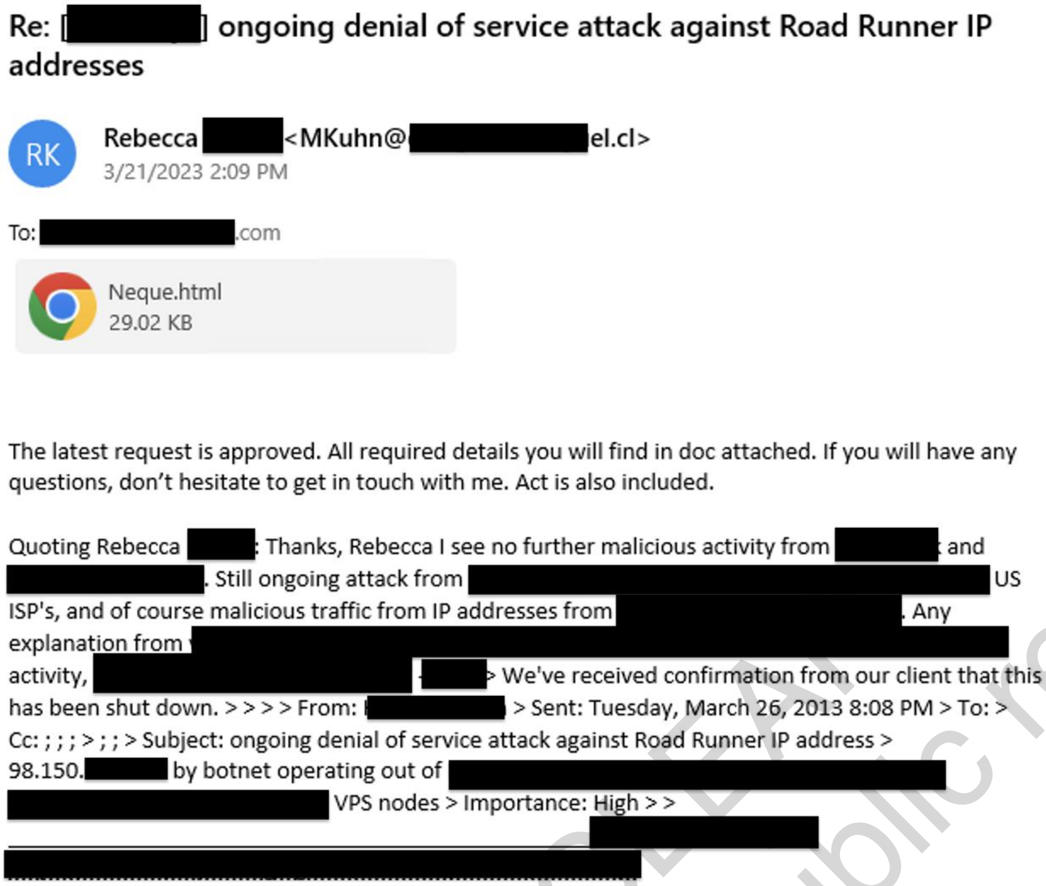
Black Basta Leverages Qakbot Email Thread Hijacking for Initial Access

Since 2020, Qakbot botnet campaigns have employed emails that were stolen from previous Qakbot infections and used to enable Qakbot-leveraging adversaries like Black Basta to launch what is called "thread hijacking" on high-value target email addresses found in the previously stolen emails.[3][4][5] Dragos assesses with moderate confidence that this tactic may facilitate Black Basta's inter-organization escalation from a lesser-value compromised organization to a not-yet-compromised higher-value organization. The Qakbot email-sending process may include a stolen but otherwise legitimate email message body with senders and recipients in the message, and a malicious link or attachment sent to one of the recipients or senders from the stolen email. This adds legitimacy to what might otherwise be a random phishing email and likely contributes to Qakbot's continued use as an initial access mechanism for Black Basta.

Network defenders and potentially targeted staff should be educated about thread hijacking and the potential for an adversary to use content from previous email threads with external organizations in their email phishing campaigns. A source provided Dragos with a sample of a Qakbot thread hijacking malicious phishing email (Figure 1) with email thread content from 10 years ago. An analysis showed a lengthy delivery chain from the HyperText Markup Language (HTML) attachment as shown in the screenshot → browser Pop-Up → HTML Smuggling → Zip file → Password → IMG file → LNK file → CMD file → REG file → Windows script file (WSF) → PowerShell → Qakbot dynamic link library (DLL) file, which is then executed with rundll32.exe.

TLP:CLEAR
Approved for public release

[2] Dragos Industrial Ransomware Analysis: Q2 2022 – Dragos Blog
[3] Qakbot Malware Now Exfiltrating Emails for Sophisticated Thread Hijacking Attacks - Kroll
[4] The First Step: Initial Access Leads to Ransomware - Proofpoint
[5] Crime Finds a Way: The Evolution and Experimentation of the Cybercrime Ecosystem - Proofpoint



Re: [[redacted]] ongoing denial of service attack against Road Runner IP addresses

Rebecca [redacted] <MKuhn@[redacted]el.cl>
3/21/2023 2:09 PM

To: [redacted].com

Neque.html
29.02 KB

The latest request is approved. All required details you will find in doc attached. If you will have any questions, don't hesitate to get in touch with me. Act is also included.

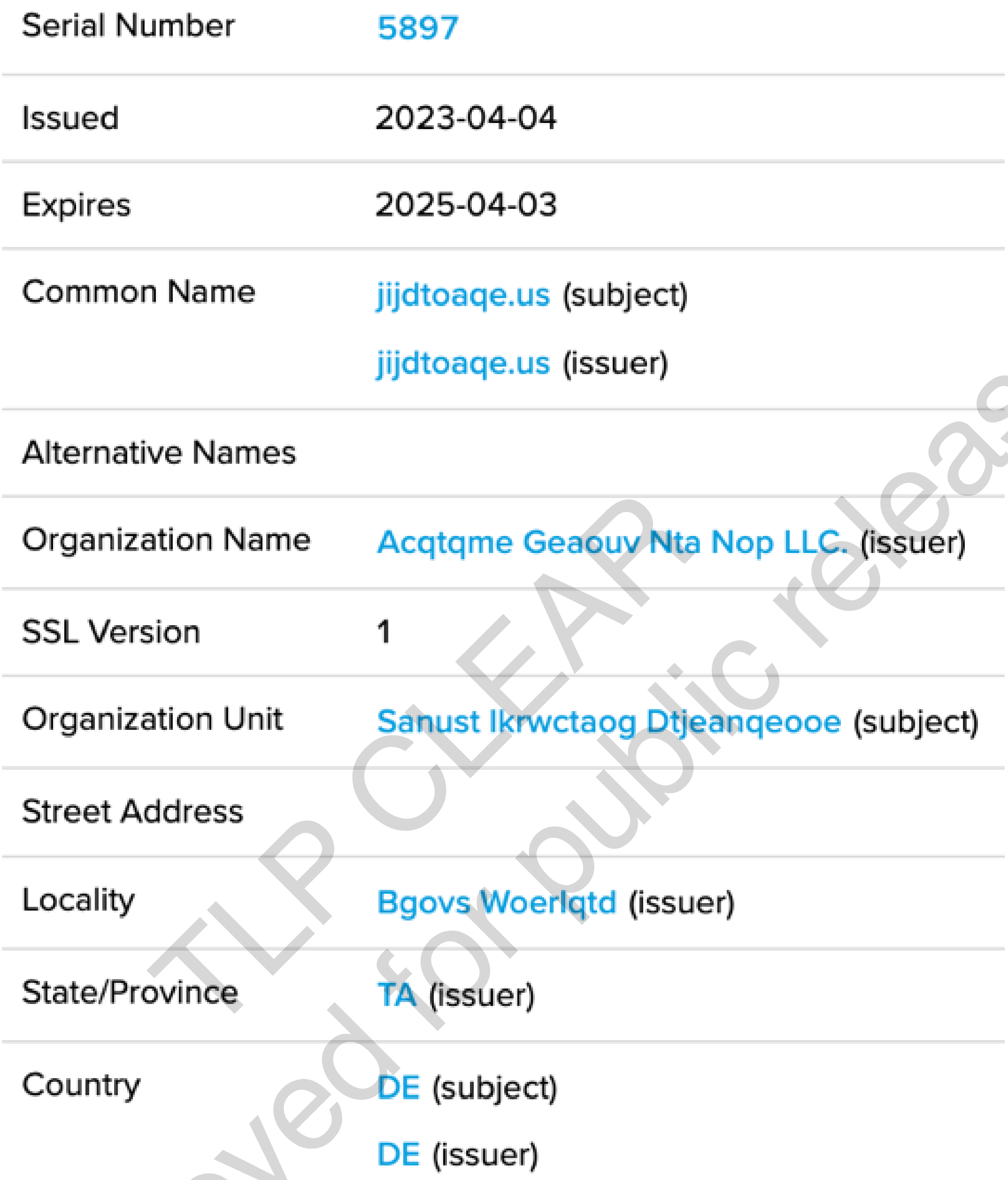
Quoting Rebecca [redacted]: Thanks, Rebecca I see no further malicious activity from [redacted] and [redacted]. Still ongoing attack from [redacted] US ISP's, and of course malicious traffic from IP addresses from [redacted]. Any explanation from [redacted] activity, [redacted] [redacted] > We've received confirmation from our client that this has been shut down. > > > > From: [redacted] > Sent: Tuesday, March 26, 2013 8:08 PM > To: > Cc: ; ; ; > ; ; > Subject: ongoing denial of service attack against Road Runner IP address > 98.150.[redacted] by botnet operating out of [redacted] VPS nodes > Importance: High > > [redacted]

FIGURE 1: EXAMPLE OF QAKBOT EMAIL THREAD HIJACKING PHISHING MESSAGE FROM MARCH 2023 QAKBOT CAMPAIGN

TLP:CLEAR
Approved for public release

Black Basta Leverages Qakbot Command and Control (C2) with Self-Signed Certificates

Since Qakbot is reportedly the most common initial access infection for Black Basta ransomware attacks, ICS and IT network defenders should employ detection and preferably web filtering regimes for common Qakbot C2 characteristics, specifically for self-signed certificates. While analyzing the internet telemetry of dozens of Black Basta victims, Dragos observed the following self-signed certificate (Figure 2) used for Qakbot C2 on a renewable energy investment firm. Note the nonsensical or partially randomized characters of the certificate name fields.



Serial Number	5897
Issued	2023-04-04
Expires	2025-04-03
Common Name	jijdtoaqe.us (subject) jijdtoaqe.us (issuer)
Alternative Names	
Organization Name	Acqtqme Geaouv Nta Nop LLC. (issuer)
SSL Version	1
Organization Unit	Sanust Ikrwctaog Dtjeanqeooe (subject)
Street Address	
Locality	Bgovs Woerlqtd (issuer)
State/Province	TA (issuer)
Country	DE (subject) DE (issuer)

FIGURE: 2 SELF-SIGNED CERTIFICATE USED FOR QAKBOT C2 WITH RENEWABLE ENERGY INVESTMENT FIRM

TLP CLEAR
Approved for public release

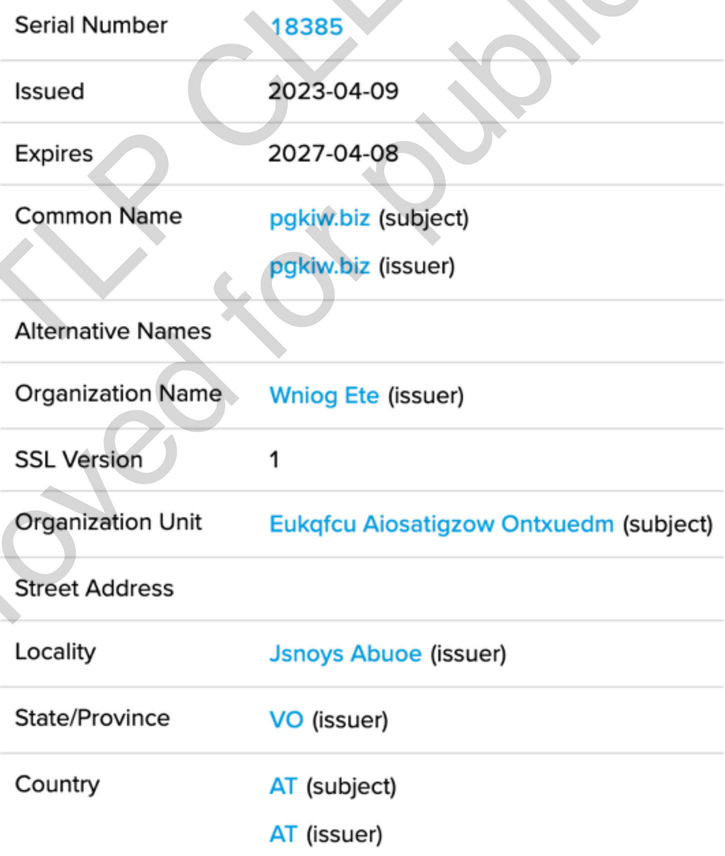
Table 1 below shows the telemetry timeline of Qakbot C2 to the eventual data exfiltration and then the presumed encryption by Black Basta actors of the renewable energy investment firm.

TABLE 1: INVESTMENT FIRM QAKBOT C2 TO BLACK BASTA EXFILTRATION TIMELINE

Renewable Energy Investment Firm Qakbot to Exfiltration Timeline	
First Qakbot C2	04/05/2023 20:29:29
Exfiltration begin	4/10/2023 20:02:04
Exfiltration end	4/11/2023 10:12:00
Total time between initial C2 and exfiltration end	5d, 13h, 42m

TLP CLEAR - Approved for public release

Similarly, Dragos observed internet telemetry for Qakbot C2 in communication with a European pharmaceutical manufacturer. This Qakbot C2 employed a different self-signed certificate with nonsensical or partially randomized characters of the certificate name fields (Figure 3).



Serial Number	18385
Issued	2023-04-09
Expires	2027-04-08
Common Name	pgkiw.biz (subject) pgkiw.biz (issuer)
Alternative Names	
Organization Name	Wniog Ete (issuer)
SSL Version	1
Organization Unit	Eukqfcu Aiosatigzow Ontxuedm (subject)
Street Address	
Locality	Jsnoys Abuoe (issuer)
State/Province	VO (issuer)
Country	AT (subject) AT (issuer)

FIGURE 3: SELF-SIGNED CERTIFICATE USED FOR QAKBOT C2 WITH EUROPEAN PHARMACEUTICAL MANUFACTURER

The initial Qakbot C2 with the European pharmaceutical manufacturer network occurred two weeks before the exfiltration and the presumed encryption by the Black Basta adversary (Table 2).

TABLE 2: MANUFACTURER QAKBOT C2 TO BLACK BASTA EXFILTRATION TIMELINE

European Pharmaceutical Manufacturer Qakbot to Exfiltration Timeline	
First Qakbot C2	04/12/2023 07:03:10
Exfiltration begin	4/25/2023 20:56:58
Exfiltration end	4/26/2023 20:20:00
Total time between initial C2 and exfiltration end	14d, 13h, 17m

Dragos proposes that these adversary activity temporal windows represent significant opportunities for critical network defenders to detect adversary C2 and disrupt Black Basta's potential operations-impacting encryption phase.

Black Basta Employs Self-Signed TLS Certificates on Exfiltration Infrastructure

Dragos assesses with moderate confidence that Black Basta employs telltale self-signed TLS certificates on data exfiltration infrastructure associated with 40% or more of all their data exfiltration targets identified since October 2022. While in almost all cases, these TLS certificates are crafted specifically for each exfiltration target, all TLS certificates of this Black Basta tactic cluster share the same fields as enumerated in Table 3. Note the blank or null Common Name and Alternative Names fields.

TLP:CLEAR
Approved for public release

TABLE 3: BLACK BASTA EXFILTRATION INFRASTRUCTURE TLS CERTIFICATE FIELDS

Issuer Distinguished Name (DN)	Subject Distinguished Name (DN)	Common Name	Alternative Names
C=GB, ST=London, L=London, O=Global Security, OU=IT Department	C=GB, ST=London, L=London, O=Global Security, OU=IT Department		

Dragos highly recommends critical network owners allow and/or filter communication to hosts with self-signed certificates only by exception. Filtering outbound communication to only allowed known categories of hosts and sites can further harden against Black Basta and other ransomware actor's use of SystemBC[6] proxy malware. Additional information on Black Basta exfiltration operations is available in TR-2023-07: Analysis of Black Basta Ransomware Exfiltration Operations[7].

Black Basta Performs C2 and Exfiltration Over DNS

Black Basta is known to deploy the Cobalt Strike penetration testing framework with a DNS Beacon feature[8] after establishing initial access. The DNS Beacon feature may be the least likely to be detected or blocked of all the Cobalt Strike C2 modules because it blends in with the voluminous DNS traffic that is typically encountered on enterprise networks. Dragos cybersecurity assessment engagements show that DNS is commonly unrestricted, even in ICS and OT networks. Dragos Platform Knowledge Packs KP-2023-003 and later provide the latest detections for DNS tunnels, including DNS tunnels used by Cobalt Strike DNS Beacon for both C2 and exfiltration. Cobalt Strike-enabled DNS tunnels are typically characterized by anomalously large volumes of TXT record queries in a short time.

The IOC section of this report includes a cluster of recently employed Cobalt Strike DNS Beacon C2 domains that intersect with Black Basta C2 domain registration tactics.

Black Basta Detection of Last Resort

According to Endpoint Detection and Response (EDR) company SentinelOne, Black Basta disables antivirus software and is known to deploy advanced EDR-evading tools.[9] Since Black Basta invariably achieves administrative privileges on their target networks to execute the encryption phase successfully, it is plausible that Black Basta can disable Data Loss Prevention (DLP) capabilities using those same administrative privileges. A DLP capability can otherwise potentially detect data being exfiltrated from a target network but is not foolproof and requires significant configuration and tuning effort, in addition to ensuring that the adversary does not evade or turn it off. One possible backstop against DLP evasion is using simple bandwidth monitoring tools to detect anomalous outbound flow (Figure 4).

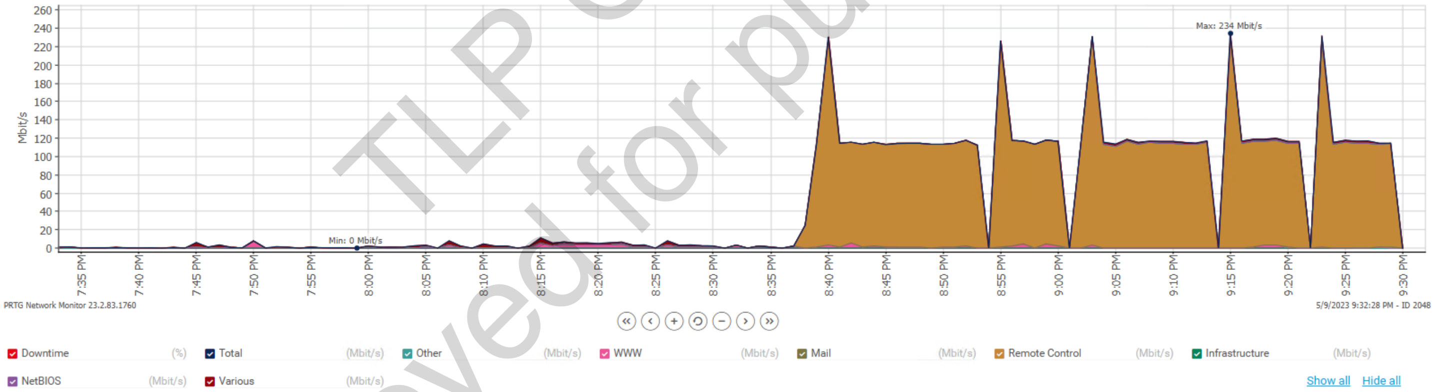


FIGURE 4: BANDWIDTH MONITORING TOOL USED TO DETECT ANOMALOUS OUTBOUND DATA FLOW

TLP CLEAR
Approved for public release

[6] SystemBC - Malpedia
[7] TR-2023-07: Analysis of Black Basta Ransomware Exfiltration Operations - Dragos WorldView
[8] DNS Beacon – Help Systems
[9] Black Basta Ransomware | Attacks Deploy Custom EDR Evasion Tools Tied to FIN7 Threat Actor - SentinelOne

Ideally, bandwidth monitoring tools should be human-monitored or instrumented for real-time alerts 24 hours a day, seven days a week.

For more details on how a Managed Security Service Provider (MSSP) successfully detected and stopped a Black Basta attack while in progress, read "Thwarting Black Basta – Case Study[10]" by Quadrant Information Security.

Black Basta ICS Impact

Dragos is unaware if Black Basta compromised or attempted to compromise OT and ICS networks related to ABB or other large organizations with ICS and OT networks. However, Black Basta has clearly demonstrated the ability to significantly disrupt operations on the critical networks of other large industrial targets besides ABB, including AGCO, Aurubis, Dole Food, and Kenworth. Black Basta, therefore, represents a capable and present threat to industrial organizations in Western Europe and North America.

Indicators of Compromise

netwsystem[.]net

steasteel[.]net

mentisys[.]net

stormsystem[.]net

quantumorbitledger[.]com

audsomsystem[.]net

snypstory[.]net

ternstreeam[.]net

netwinmontana[.]net

sysroomamd[.]net

boostmazer[.]net

sytemstern[.]net

potistream[.]net

geomandom[.]net

resysmon[.]net

filestorsmy[.]com

TLP CLEAR
Approved for public release

[10] Thwarting Black Basta Case Study - Quadrant Information Security

Mitigations

Host

- Employ separate authentication infrastructure for ICS and OT networks from enterprise networks.

Network

- In ICS and OT networks, block internet-communicating DNS protocols when practical, or allow only by exception.
- Filter outbound connections to known-good or categorized hosts.

Detections

Apply Dragos Knowledge Pack (KP) KP-2023-003 or later. The following Dragos Platform notifications alert on DNS-based tunnels consistent with the Cobalt Strike Malleable C2 DNS Beacon used by Black Basta.

- DNS TXT Queries High Volume - Possible DNS Tunnel
- DNS TXT Max Size Responses - Possible DNS Tunnel

Recommendations

- Consider restricting internet traffic in ICS, OT, and critical-to-operations IT environments to only categorized or known good hosts by using web filtering or allowing only by exception.
- Allow communication with hosts using self-signed TLS certificates only by exception.
- Apply the latest Dragos Platform Knowledge Pack and otherwise monitor for anomalously large volumes of DNS TXT record queries on the ICS, OT, and IT networks that are critical for operations.
- Alert and block communication with the domain IOCs in this advisory.
- Monitor and alert for anomalous outbound data flow that is consistent with malicious data exfiltration.
- Implement mitigations for Black Basta TTPs listed in the Appendix.
- Implement relevant critical controls for ICS and OT[11].
- Design, refine, implement, and rehearse ransomware response plans across the organization and with external organizations that have critical roles in operations.

Conclusion

Black Basta's recent attack on the large industrial equipment and service provider ABB illustrates the potential impacts and risks to multiple industries from a capable ransomware adversary. Dragos has proposed and described five strongly recommended Black Basta tactics for network defenders' counter-adversary efforts. Implement detection, mitigation, and hunting efforts for these Black Basta tactics on ICS, OT, and operation-critical IT networks.

TLP CLEAR
Approved for public release

[11] Five Critical Controls for OT Cybersecurity - Emerson

References

- AGCO Ransomware Incident – Dragos WorldView
- Dragos Industrial Ransomware Analysis: Q2 2022 – Dragos Blog
- Multinational tech firm ABB hit by Black Basta ransomware attack – BleepingComputer
- Hitachi Energy Ltd cancels shifts, halts manufacturing, blames IT service disruption - KRCG TV
- Qakbot Malware Now Exfiltrating Emails for Sophisticated Thread Hijacking Attacks - Kroll
- The First Step: Initial Access Leads to Ransomware - Proofpoint
- Crime Finds a Way: The Evolution and Experimentation of the Cybercrime Ecosystem - Proofpoint
- TR-2023-07: Analysis of Black Basta Ransomware Exfiltration Operations - Dragos WorldView
- DNS Beacon - Help Systems
- Thwarting Black Basta Case Study - Quadrant Information Security
- SystemBC - Malpedia
- Five Critical Controls for OT Cybersecurity - Emerson
- Black Basta Ransomware | Attacks Deploy Custom EDR Evasion Tools Tied to FIN7 Threat Actor - SentinelOne

TAGS: Ransomware, Black Basta, TA577, Qakbot, Qbot, Cobalt Strike, DNS Tunnel, Exfiltration, SSH, Secure Shell, FIN7, Thread Hijacking, Automobile, Manufacturing, Defense Industrial, Energy, Utility, Equipment Rental, Food & Beverage, Industrial & Utility Construction, Industrial Distribution, Industrial Machinery, Industrial Manufacturing, Industrial Metals, Metals and Mining, Industrial Transport, Marine Engineering, Pharmaceutical, Plastic Technology, Rail, Textiles, Europe, North America, IR-043-2022, IR-007-2022, IR-008-2022, IR013-2022, IR-021-2022, IR-025-2022, IR-033-2022, IR-038-2022, IR-039-2022, IR-40-2022

TLP CLEAR
Approved for public release

Appendix – Black Basta MITRE Enterprise ATT&CK Mapping

Tactic	Technique
Resource Development	T1584.005 - Compromise Infrastructure: Botnet
Resource Development	T1586.002 - Compromise Accounts: Email Accounts
Initial Access	T1566.001 - Phishing: Spearphishing Attachment
Initial Access	T1566.002 - Phishing: Spearphishing Link
Initial Access, Privilege Escalation, Defense Evasion, Persistence	T1078 - Valid Accounts
Execution	T1059.003 - Command and Scripting Interpreter
Execution	T1569.002 - System Services: Service Execution
Execution	T1047 - Windows Management Instrumentation
Privilege Escalation	T1068 - Exploitation for Privilege Escalation
Defense Evasion, Privilege Escalation	T1484.001 - Domain Policy Modification: Group Policy Modification
Defense Evasion	T1112 - Modify Registry
Defense Evasion	T1562.001 - Impair defenses: Disable or Modify Tools
Credential Access	T1003 - OS Credential Dumping
Discovery	T1082 - System Information Discovery
Discovery	T1018 - Remote System Discovery
Discovery	T1083 - File and Directory Discover
Command and Control	T1071.001 - Application Layer Protocol: Web Protocols
Command and Control	T1071.004 - Application Layer Protocol: DNS
Lateral Movement	T1570 - Lateral Tool Transfer
Lateral Movement	T1021.001 - Remote Services: Remote Desktop Protocol
Exfiltration	T1020 - Automated Exfiltration
Exfiltration	T1041 - Exfiltration Over C2 Channel
Exfiltration	T1567 - Exfiltration Over Web Service
Impact	T1490 - Inhibit System Recovery
Impact	T1489 - Service Stop
Impact	T1486 - Data Encrypted for Impact
Impact	T1491 - Defacement

TLP CLEAR
Approved for public release