Deconstructing a Cybersecurity Event

dragos.com/blog/deconstructing-a-cybersecurity-event/

May 10, 2023

Blog Post

By Dragos, Inc.

05.10.23

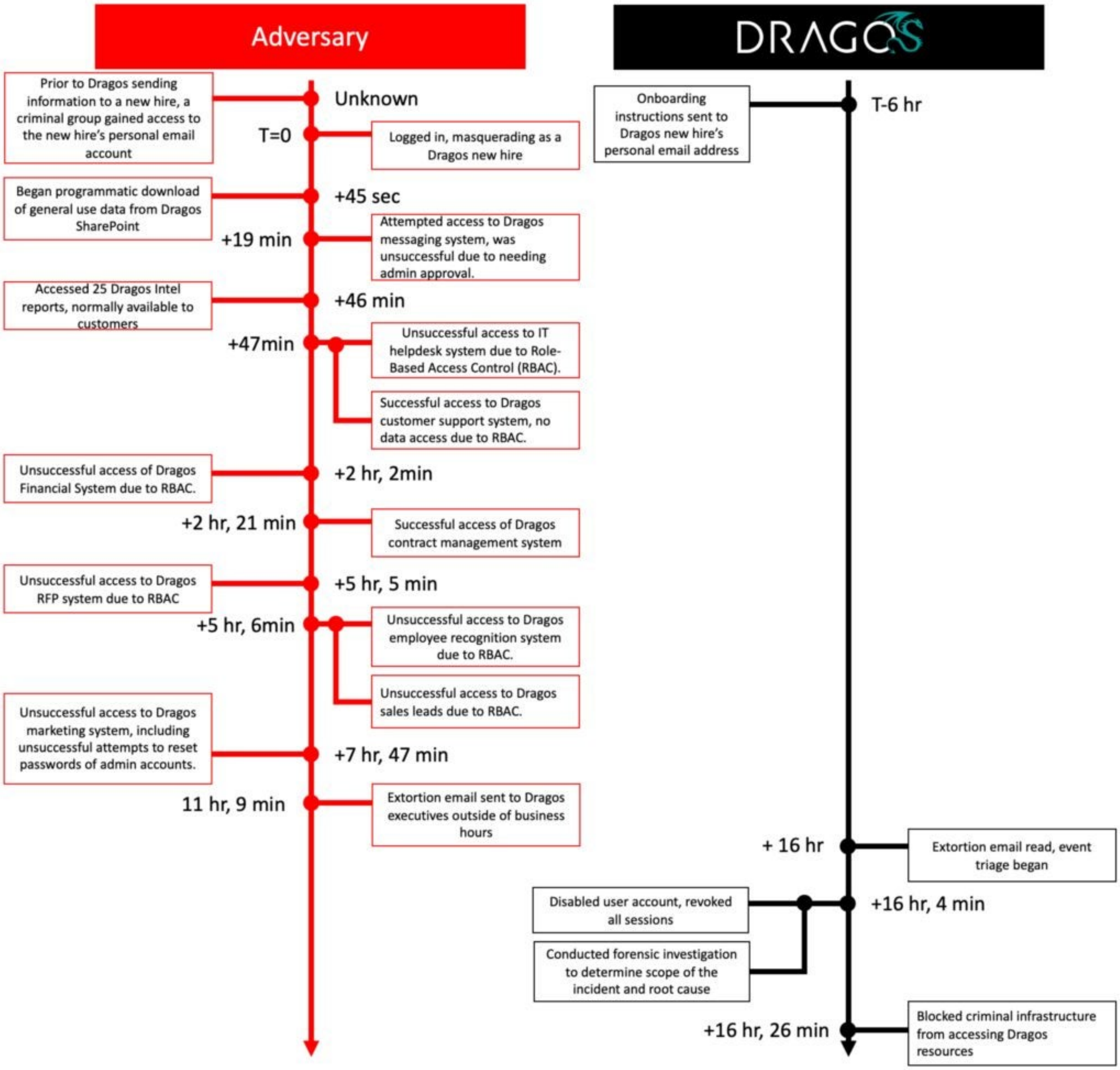
On May 8, 2023, a known cybercriminal group attempted and failed at an extortion scheme against Dragos. No Dragos systems were breached, including anything related to the Dragos Platform.

Dragos has a culture of transparency and a commitment to providing educational material to the community. This is why it's important to us to share what happened during a recent failed extortion scheme against Dragos in which a cybercriminal group attempted to compromise our information resources. We want to share this experience with the community, describe how we prevented it from being much worse, and, hopefully, help de-stigmatize security events.

The criminal group gained access by compromising the personal email address of a new sales employee prior to their start date, and subsequently used their personal information to impersonate the Dragos employee and accomplish initial steps in the employee onboarding process. The group accessed resources a new sales employee typically uses in SharePoint and the Dragos contract management system. In one instance, a report with IP (internet protocol) addresses associated with a customer was accessed, and we've reached out to the customer.

We investigated alerts in our corporate Security Information & Event Management (SIEM) and blocked the compromised account. We promptly activated our incident response retainer with Crowdstrike and engaged our third-party Monitoring, Detection & Response (MDR) provider to manage incident response efforts. We are confident that our layered security controls prevented the threat actor from accomplishing what we believe to be their primary objective of launching ransomware. They were also prevented from accomplishing lateral movement, escalating privileges, establishing persistent access, or making any changes to the infrastructure.

Timeline



Adversary

Unknown: Prior to Dragos sending information to a new hire, a criminal group gained access to the new hire's personal email account

T=0: Logged in, masquerading as a Dragos new hire

+45 sec: Began programmatic download of general use data from Dragos SharePoint

+19 min: Attempted access to Dragos messaging system, was unsuccessful due to needing admin approval.

+46 min: Accessed 25 Dragos Intel reports, normally available to customers

+47min: Unsuccessful access to IT helpdesk system due to Role-Based Access Control (RBAC).

Successful access to Dragos customer support system, no data access due to RBAC.

+2 hr, 2min: Unsuccessful access of Dragos Financial System due to RBAC.

+2 hr, 21 min: Successful access of Dragos contract management system

+5 hr, 5 min: Unsuccessful access to Dragos RFP system due to RBAC

+5 hr, 6min: Unsuccessful access to Dragos employee recognition system due to RBAC.

Unsuccessful access to Dragos sales leads due to RBAC.

+7 hr, 47 min: Unsuccessful access to Dragos marketing system, including unsuccessful attempts to reset passwords of admin accounts.

11 hr, 9 min: Extortion email sent to Dragos executives outside of business hours

DRAGOS

T-6 hr: Onboarding instructions sent to Dragos new hire's personal email address

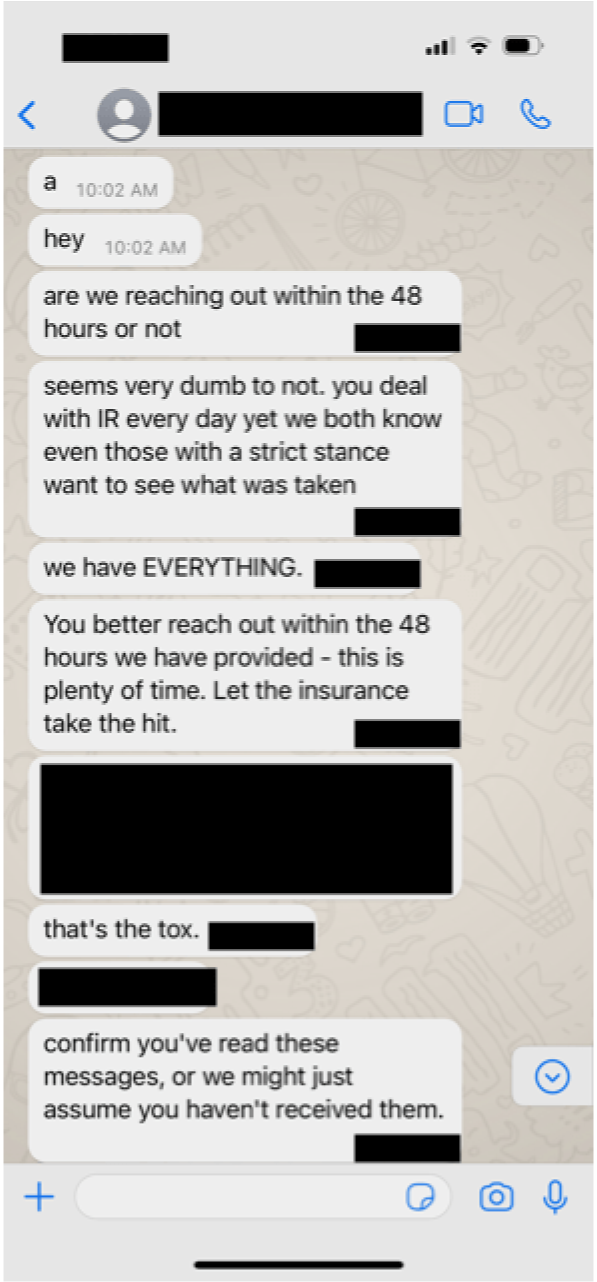
+ 16 hr: Extortion email read, event triage began

+16 hr, 4 min: Disabled user account, revoked all sessions

Conducted forensic investigation to determine scope of the incident and root cause

+16 hr, 26 min: Blocked criminal infrastructure from accessing Dragos resources

A known TTP of this criminal group is to deploy ransomware. After they failed to gain control of a Dragos system and deploy ransomware, they pivoted to attempting to extort Dragos to avoid public disclosure. Below are samples of various messages sent to Dragos executives.



[redacted]

[redacted]

a 10:02 AM

hey 10:02 AM

are we reaching out within the 48 hours or not [redacted]

seems very dumb to not. you deal with IR every day yet we both know even those with a strict stance want to see what was taken [redacted]

we have EVERYTHING. [redacted]

You better reach out within the 48 hours we have provided - this is plenty of time. Let the insurance take the hit. [redacted]

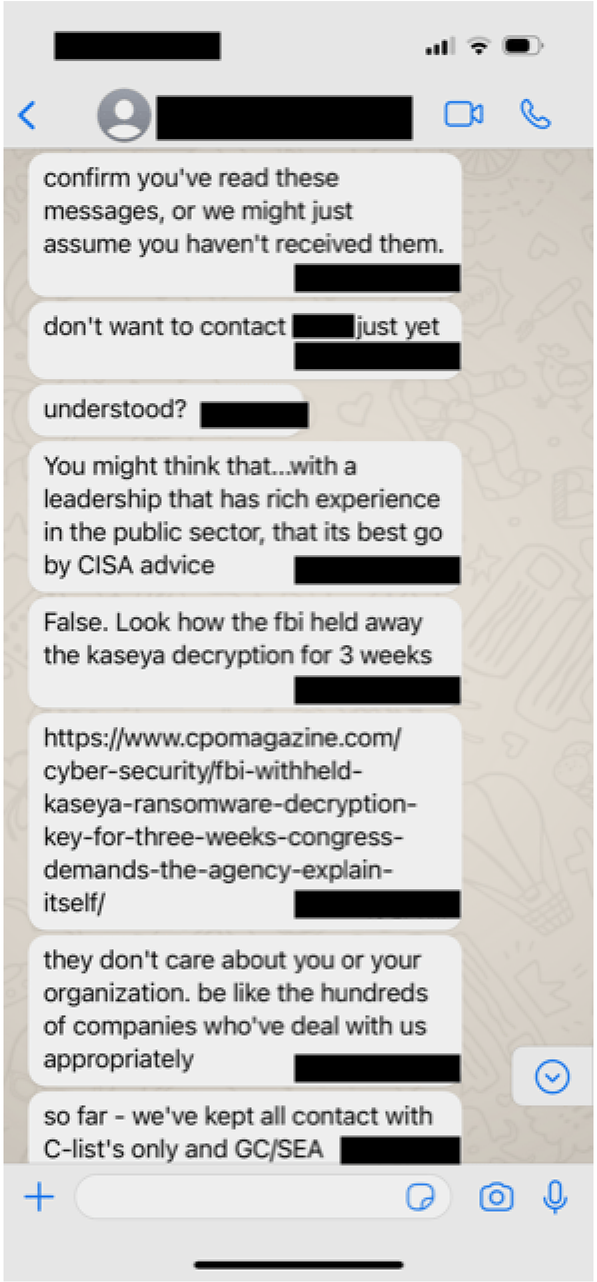
[redacted]

that's the tox. [redacted]

[redacted]

confirm you've read these messages, or we might just assume you haven't received them. [redacted]

The next activity was to expand tactics to include references to family members and contacts.



[redacted]

[redacted]

confirm you've read these messages, or we might just assume you haven't received them. [redacted]

don't want to contact [redacted] just yet [redacted]

understood? [redacted]

You might think that...with a leadership that has rich experience in the public sector, that its best go by CISA advice [redacted]

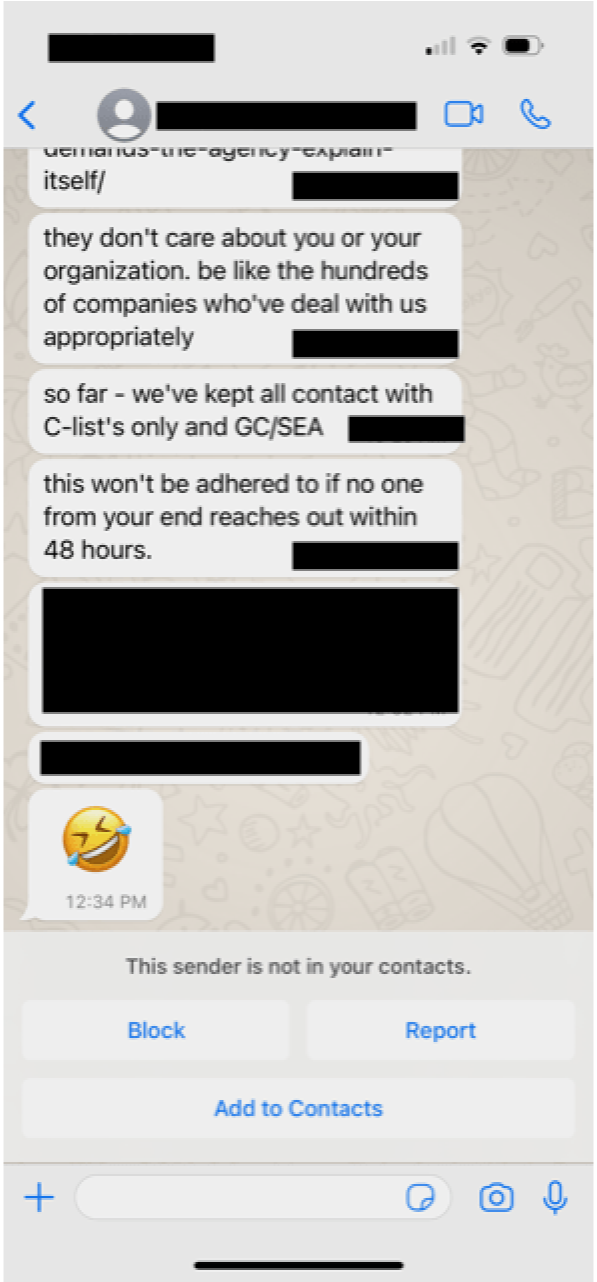
False. Look how the fbi held away the kaseya decryption for 3 weeks [redacted]

https://www.cpomagazine.com/cyber-security/fbi-withheld-kaseya-ransomware-decryption-key-for-three-weeks-congress-demands-the-agency-explain-itself/ [redacted]

they don't care about you or your organization. be like the hundreds of companies who've deal with us appropriately [redacted]

so far - we've kept all contact with C-list's only and GC/SEA [redacted]

The cybercriminal continued to escalate their messages, Dragos did not engage.



[redacted]

[redacted]

demands-the-agency-explain-itself/ [redacted]

they don't care about you or your organization. be like the hundreds of companies who've deal with us appropriately [redacted]

so far - we've kept all contact with C-list's only and GC/SEA [redacted]

this won't be adhered to if no one from your end reaches out within 48 hours. [redacted]

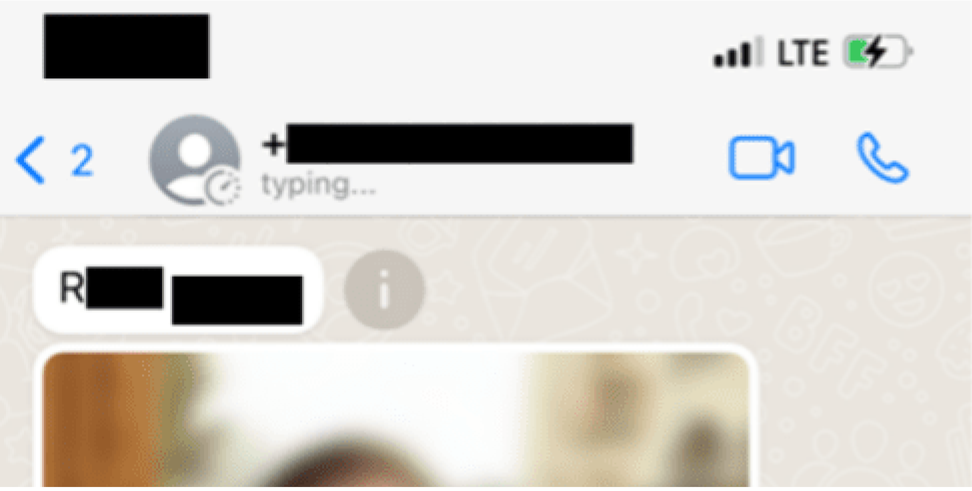
[redacted]

[redacted]

🤣 12:34 PM

This sender is not in your contacts.

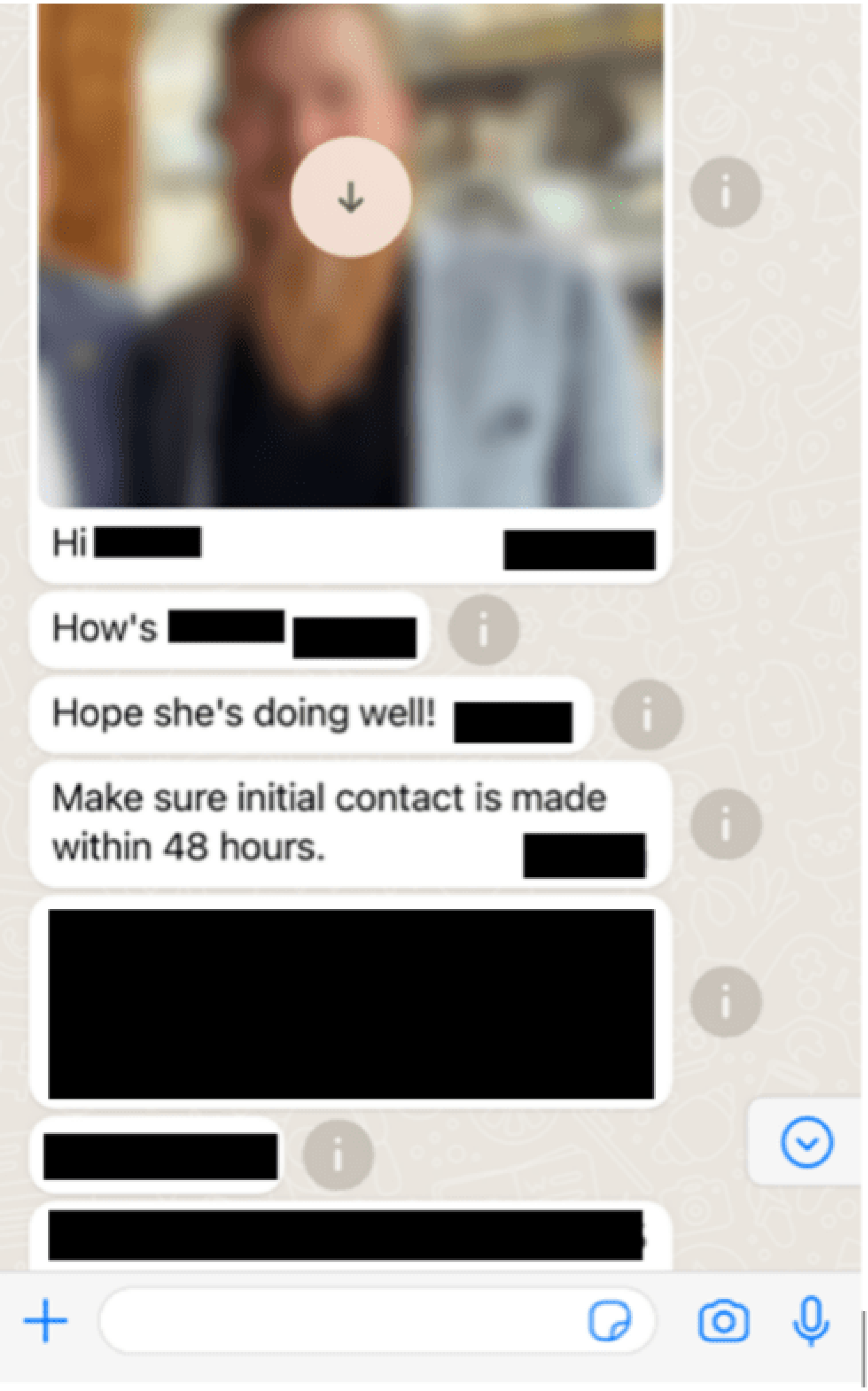
The cybercriminal continued reaching out to multiple publicly known Dragos contacts to elicit a response.



[redacted]

+[redacted]
typing...

R[redacted]



Hi [redacted] [redacted]

How's [redacted] [redacted]

Hope she's doing well! [redacted]

Make sure initial contact is made within 48 hours. [redacted]

[redacted]

[redacted]

[redacted]

The cybercriminal's texts demonstrated research into family details as they knew names of family members of Dragos executives, which is a known TTP. However, they referenced fictitious email addresses for these family members. In addition, during this time, the cybercriminal contacted senior Dragos employees via personal email.

Our decision was that the best response was to not engage with the criminals.

While the external incident response firm and Dragos analysts feel the event is contained, this is an ongoing investigation. The data that was lost and likely to be made public because we chose not to pay the extortion is regrettable. However, it is our hope that highlighting the methods of the adversary will help others consider additional defenses against these approaches so that they do not become a victim to similar efforts.

MITRE ATT&CK Mapping

Tactic	Technique	Procedure
TA0001	T1078	Leverage Valid Accounts
TA0006	T1621	Multi-Factor Authentication Request Generation
TA0007	T1526	Cloud Service Discovery
TA0009	T1530	Collect Data from Cloud Storage
TA00010	T1567	Exfiltration Over Web Service
TA0042	T1586.002	Compromise Email Accounts
TA0043	T1593	Search Open Websites/Domains
	T1591.004	Gather Victim Org Information: Identify Roles

Indicators of Compromise

IP Addresses

`144[.]202[.]42[.]216`

`162[.]33[.]179[.]126`

Email Address

`dragos.negotiations[@]proton.me`

Lessons Learned

In response to this event, we added an additional verification step to further harden our onboarding process and ensure that this technique cannot be repeated.

Every thwarted access attempt was due to multi-step access approval. We are evaluating expanding the use of this additional control based on system criticality.

Positive outcomes further reinforce our resolve to not engage or negotiate with cybercriminals.

Verbose system activity logs enabled the rapid triage and containment of this security event.

Recommendations

- Harden Identity & Access Management infrastructure and processes
- Implement separation of duties across the enterprise
- Apply the principle of least privilege to all systems and services
- Implement multi-factor authentication everywhere feasible
- Apply explicit blocks for known bad IP addresses (like those shown above)
- Scrutinize incoming emails for typical phishing triggers, including the email address, URL, and spelling
- Ensure continuous security monitoring is in place, with tested incident response playbooks

Again, our investigation is ongoing, and we will reach out directly if we learn of additional effects on our customers. In the meantime, if you have questions, please send them to Dragos's Office of the CISO at ciso-office@dragos.com.