IPTOR SECURITY INCIDENT

Customer Q&A

November 2023

Document Version 1.0 (Issue)

IPTOR SECURITY INCIDENT Customer Q&A

November 2023

1. DISCLAIMER

This document in any form (electronic, printed, imaged or other), contains proprietary information that is the exclusive property of Iptor. Your access to, and use of this confidential material is subject to the terms and conditions of your Iptor Master Software Agreement (MSA), Software Licence and Services Agreement (SLSA) and all other Agreements that have been executed and are party to our Commercial relationship and to which you agree to adhere to.

This document and information contained herein may not be copied, reproduced, distributed or copied outside of Iptor and your contracted entities without the express prior written consent by Iptor.

This document does not formulate any contractual agreement with Iptor or its subsidiaries and affiliates and is for information and guidance only. Any statements made herein regarding product direction (Iptor or Third Party) should not be implied as a reliance to make purchasing or other strategic directional choices within your organization. Nothing herein constitutes a commitment to any timings, versioning, release or development of any specific features and functions which remain at the sole discretion of Iptor in terms of commitment, delivery and timing.

2. VERSION CONTROL

1.1	14 Nov 2023	18:00 CET	Update
1.0	07 Nov 2023	18:00 CET	Initial Issue

3. INCIDENT INFORMATION

1.1 INCIDENT SUMMARY

At 11.03am (CET), Saturday 4th November Iptor Corporate systems were targeted by an Akira Ransomware attack and a ransomware demand was received. High CPU activity was detected across several servers indicating threat activity along with elements of network peaking. Iptor's containment response commenced no later than 11:30am (CET).

1.2 WHAT WAS THE CONTAINMENT AND IMMEDIATE RESPONSE?

In order to contain exposure and prevent any proliferation external to Iptor's Corporate network our VPNs and external network connections were both disabled and shut down by 12:30 CET and our CATOs were disabled by 17:02 CET. At this point the Iptor Corporate network was in total isolation from all external networks. Forensic investigation started immediately with our internal and cybersecurity partners conducting checks on all Customer environments and Internal environments and is on-going until all systems are validated and verified.

1.3 WHAT SYSTEMS/SERVICES WERE COMPROMISED AND WHAT DATA WAS AT RISK?

A number of internal Corporate Iptor systems and services were impacted. Investigations are at an early stage and Iptor is still progressing the forensic investigation in order to determine the scope and impact of the incident on the systems and data.

1.4 WHAT SYSTEMS/SERVICES WERE SUSPENDED?

Iptor limited all services that require network connectivity including (but not limited to) our DNS servers, VPN servers, CATO servers along with suspending all employee access to the corporate network.

1.5 IS IPTOR IN PARTNERSHIP WITH REGARDS THIS INCIDENT?

Iptor is working with numerous external partners including cyber security and forensic IT specialists. At this time, we are unable to disclose those partners.

1.6 DO YOU KNOW THE THREAT ACTOR AND/OR HAVE ANY ATTRIBUTION TO THE THREAT ACTOR?

Based on current evidence this incident is attributed to Akira Ransomware Group as the Threat Actor.

1.7 WHAT IS THE STATUS OF ANY FORENSIC ANALYSIS?

Our forensic analysis will continue until each and every system and operating entity/element within, connected to (either permanently or intermittently) to Iptor's Corporate network has been validated, verified and assured for its integrity. It is a complex process that is expected to take some time.

4. STATUTORY NOTIFICATION, REGULATION AND INFORMATION

1.8 HAVE THE RELEVANT DATA PROTECTION AUTHORITIES (DPA) (E.G. RELATING TO GDPR) BEEN NOTIFIED?

Relevant authorities have been (or are in the process of being) notified within the required timeframe once the required information was collated in order to submission definitions of each Authority. Iptor is conscious of its regulatory obligations and will continue to assess its reporting obligations as further information becomes available.

1.9 CAN END-CUSTOMERS AND PARTNERS RECEIVE COPIES OF THE DPA NOTICES?

Iptor will not be providing copies of any notifications made to any DPAs.

1.10 HAVE ANY LAW ENFORCEMENT AGENCIES BEEN NOTIFIED?

It is not appropriate for Iptor to comment on the engagement of any such Agencies at this time.

1.11 HAS AN EXTERNAL LAW FIRM BEEN APPOINTED?

Iptor has its own General Council who are the central point for legal matters in regards to any Iptor Corporate incident. At the same time, we have engaged lawyers from our Group Company Genii-GSG who in turn have specialist external lawyers providing oversight of this matter. We are not at liberty to name this law firm at this time.

1.12 WHAT LEGAL REPORTING DO I HAVE TO EXECUTE AS A CUSTOMER/PARTNER?

Iptor is not in a position to give guidance regarding individual customers/partners in the differing jurisdictions therefore we would advise you contact your legal and/or compliance department to understand those requirements or to seek external advice in the absence of retaining such resources in-house.

5. DATA IMPACT

1.13 WHAT DATA HAS BEEN IMPACTED?

Given the ongoing nature of the forensic investigation into the incident, Iptor is not in ap position to confirm the scope of the data that has been impacted. This analysis continues at pace and Iptor will contact any affected parties at the appropriate time in due course, depending upon the outcome of the investigation.

1.14 WHAT IS THE SCOPE / SCALE OF THE INCIDENT?

Given the ongoing nature of the forensic investigation into the incident, Iptor is not in a position to confirm the scope of the data that has been impacted. This analysis continues at pace and Iptor will contact any affected parties at the appropriate time in due course, depending upon the outcome of the investigation.

1.15 IS IPTOR THE "CONTROLLER" OR THE "PROCESSOR" IN REGARDS OF THIS INSTANCE?

This position is subject to ongoing investigation.

1.16 WHAT TYPE OF DATA WOULD YOU RETAIN IN REGARDS OF MY COMPANY THAT YOU CONTRACT WITH?

Data that is within the Iptor corporate network that is held in conjunction with our daily business operations with clients (past, present and future) is limited to the following: -

- Names, email addresses and titles relating to persons with whom Iptor for commercial or operational reasons require correspondence with in regards of our business relationship.
- Commercial items such as Contracts, NDA's, DPA's, Statement of Works, Project Plans required for the execution of new or continued business between the parties.
- Documents relating to projects and specifications such as PowerPoint presentations, RFIs, RPFs, RPQs, Specification and Requirements documents.
- Financial information such as Invoicing, Purchase Orders/Requests, Goods Received Notes, Credit Notes, Accounts Payable and Receivable.

Please note that the list above DOES NOT constitute data that has been lost, exposed or leaked in this Incident but highlights the type of customer data that is retained on our Corporate Network, Corporate Systems and/or File Servers.

6. IPTOR INITIAL TECHNICAL RESPONSES

1.17 HOW DID IPTOR PROTECT CUSTOMER SYSTEMS IN THIS INSTANCE?

Iptor has a comprehensive set of cyber security measures deployed across its IT system network in order to maintain an appropriate level of security for all systems data, one of which is to have network separation and autonomy in regards of Infrastructure & networks running systems of our Customers as opposed to those running Iptor's Corporate systems. Our forensic investigations are ongoing to assess the data involved.

1.18 WHAT HAS IPTOR DONE TO VALIDATE AND SECURE ITS CORPORATE ASSETS?

Iptor disabled all external networking and internal connectivity (including employee VPNs) in the first instance. All critical systems were shutdown to avoid any proliferation. Over time our security partners and teams are scanning, validating and reinitiating systems to bring them on¬line in an orderly and secure manner including looking for any activity or actions which may have been deployed to leave "back-doors" for the Threat Actor to then further exploit.

1.19 HOW DO I KNOW IPTOR'S STAFF LAPTOP'S ARE SAFE TO CONNECT WITH ME?

We understand that Iptor laptops have not been involved directly by the incident. However, as part of the review of our cyber security measures following the incident, we have taken additional measures to strengthen the security of our laptops by automatically:

- Updating the antivirus signature files and activated a full scan.
- Installed a Forensic and Incident Response Tool ("Velociraptor").
- Used IOC hash codes to create Hunts in Velociraptor to verify of any further compromise on the device.
- Executed a full file scan to ensure that no files with the Akira encrypted file extension are present to find and remove any unusual files.

For any active device that has not received the automated deployment, the device will be disabled remotely.

1.20 WHAT MEASURES HAS IPTOR TAKEN OR PLANS TO TAKE TO STRENGTHEN DATA SECURITY AND PREVENT FUTURE INCIDENTS?

It would not be appropriate for Iptor to divulge the full extent of the cyber security measures in place to external third parties. However, once this incident is resolved Iptor will undertake a detailed review and consider the extent to which it would be appropriate to consider additional measures.

Continues …./

7. CUSTOMER INITIAL RESPONSE

1.21 WHAT SHOULD I DO AS AN IMMEDIATE FIRST STEP BASED ON YOUR INCIDENT?

We would advise customers of the following good practice that should continually be maintained and, in instances such as this immediately reviewed, namely:

- To execute a thorough review of all ingress points to the Customer estate (including VPN Gateways) to ensure the latest level of recommended software release and patches / patch levels.
- Ensure regular anti-malware updates and scans across their entire estate.
- Ensure that the User Credential repository (e.g. LDAP) matches the users and assets that are active and that any unknown authentication entities are disabled or deleted.

A more comprehensive guide that Iptor has created can be found on the Iptor.com website at: https://iptor.com/iptor-security-update/ following the link to "Best Practices" or via:

https://25369120.fs1.hubspotusercontent-eu1.net/hubfs/25369120/Iptor%20Resources/Best%20Practice%2c%20Akira-1.pdf

8. TECHNICAL DETAILS

1.22 WHERE DO I FIND THE INDICATORS OF COMPROMISE?

In an effort to enable our customers to have a greater awareness and conduct their own assessments of their IT environments for tradecraft attributed to the Akira ransomware strain, we are sharing information already within the public domain from security threat researchers attributed to the Akira ransomware strain.

IoC's can be found at: https://iptor.com/iptor-security-update/ following the link to "IoCs"

Hash Codes provided by Iptor can be found at the same web address following: "Hash Codes"

Trend Micro's comprehensive article can be found here:

https://www.trendmicro.com/vinfo/gb/security/news/ransomware-spotlight/ransomware-spotlight-akira

9. WORKING WITH CUSTOMERS / PARTNERS

1.23 HOW WILL IPTOR WORK IN REGARDS OF STATUTORY OBLIGATIONS TO CUSTOMERS AND PARTNERS?

Iptor will work with all Customers and Partners on their specific requirements in regards of Governance and any Legal Obligations in the due course of time further to our continued recovery of operations. We welcome your patience during this time.

10. LESSONS LEARNED / NEXT STEPS

1.24 WHAT CHANGES HAVE BEEN IMPLEMENTED TO MINIMIZE THE CHANCE OF A SIMILAR ATTACK?

It would not be appropriate for Iptor to divulge the full extent of the cyber security measures in place to external third parties. However, once this incident is resolved Iptor will undertake a detailed review and consider the extent to which it would be appropriate to consider additional measures.

1.25 WHAT CHANGES ARE PLANNED BUT YET TO BE IMPLEMENTED TO PREVENT A REPEAT OF THIS ATTACK?

It would not be appropriate for Iptor to divulge the full extent of the cyber security measures in place to external third parties. However, once this incident is resolved Iptor will undertake a detailed review and consider the extent to which it would be appropriate to consider additional measures.

1.26 WILL IPTOR SHARE THE EXPERIENCES FROM START TO END IN REGARDS OF THIS SECURITY INCIDENT AT SOME TIME IN THE FUTURE?

Once this incident is resolved and normal operations have resumed, Iptor will consider the extent to which it will be able to share its knowledge and learnings of the Incident, so that customers and partners can benefit from our experience of this incident.