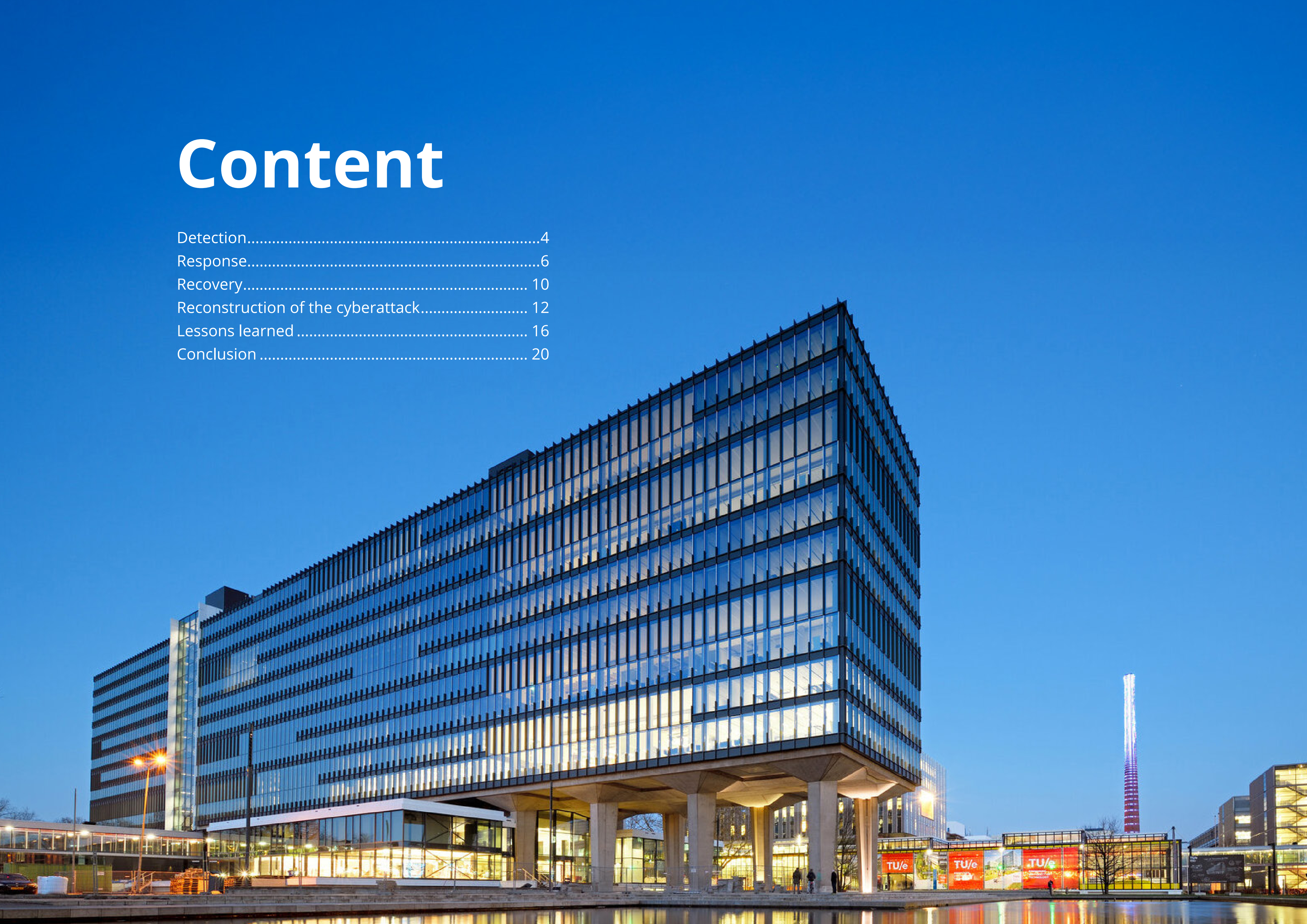
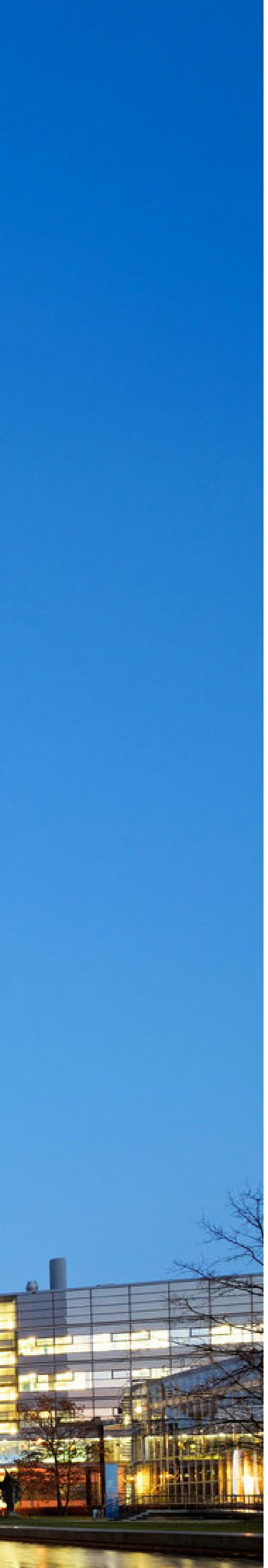
FOX IT
part of nccgroup

The TU/e cyberattack of January 2025 from Fox-IT's incident response perspective

Content





Introduction

Eindhoven University of Technology (TU/e) suffered a cyberattack in January 2025. The attack was detected in the evening of Saturday, January 11, by TU/e and SURFsoc. SURFsoc is a security monitoring service delivered by Fox-IT and managed by SURF, the collaborative organization that provides IT services and infrastructure to higher education and research institutions in the Netherlands.

Shortly after detecting the attack, TU/e started its incident response process and called in the help of Fox-IT's Computer Emergency Response Team (FoxCERT). The university also notified SURFcert, the network of incident response experts within SURF and affiliated institutions. Thanks to the rapid and decisive response actions taken by TU/e and FoxCERT during that night, the university was able to significantly reduce the impact of the attack.

No systems were destroyed, no ransomware was deployed, and the digital forensic investigation found no evidence that large amounts of data had been stolen. TU/e kept its networks offline for one week, to allow for a thorough investigation into the cyberattack, identify and address weaknesses, and prepare its IT systems for resuming normal operations. TU/e brought its systems back online and resumed business as usual operations on Monday, January 20.

Fox-IT supported TU/e throughout this period and afterwards from its position as provider of Managed Detection and Response (MDR) and Digital Forensics and Incident Response (DFIR) services. Fox-IT provided the university with support and guidance based on those two services, but it did not assess nor was it responsible for the overall cybersecurity of TU/e or the hardening of its systems.

This document describes how the cyberattack was detected and how the incident response and digital forensic investigation took place. It also presents a reconstruction of the cyberattack based on the forensic investigation and recommendations to reduce the risk of falling victim to this kind of cyberattack in the future.

Detection

TU/e makes use of the SURFsoc security monitoring service organized by SURF and delivered by Fox-IT. Around 22:00 on Saturday, January 11, SURFsoc detected suspicious activity within TU/e systems.

The Security Operations Center (SOC) analysts on duty responded by triaging the activity and identifying that a threat actor was active within TU/e systems. They assessed the nature of the threat actor's activity to indicate an imminent threat and activated the emergency procedures agreed upon with TU/e.

SURFsoc contacted TU/e by phone around 22:50, explained the situation and its urgency in detail, providing clear advice on recommended next steps. At that time TU/e was already looking into the situation because the university had received an automated detection alert from one of their tools. TU/e and the SURFsoc together engaged FoxCERT and started the emergency incident response procedures as described in the next section.

How the cyberattack was detected by both SURFsoc and TU/e

The SURFsoc service at TU/e was designed to monitor key systems within the organization's IT environment, including the Active Directory (AD) domain controllers. When the threat actor interacted with those systems to gain domain administrator privileges, SURFsoc analysts detected the activity, analysed it, and alerted TU/e to the situation and its urgency.

At that time TU/e was already gearing up for action because a vigilant member of the university's IT team had noticed an alert generated by one of their security tools half an hour before SURFsoc contacted them. Despite it being Saturday evening, that person had recognized the alert's seriousness and set the university's incident response procedure in motion.Thanks to the vigilance and swift actions of TU/e staff and the confirmation and guidance from SURFsoc, the university quickly grasped the urgency of the situation and was able to halt the cyberattack before it could cause disruptive damage, such as deploying ransomware.

Could the attack have been detected earlier?

The forensic investigation described in the next section showed that the threat actor had interacted with TU/e systems before the attack was detected. Those earlier activities were not detected because they were outside the visibility of the TU/e monitoring tools available to SURFsoc or because they mimicked legitimate user behaviour. Those activities were uncovered by the forensic investigation because that investigation had access to more data and tools than the SURFsoc monitoring service.

The attack could have been detected earlier if the scope of SURFsoc monitoring had been expanded, for example by including network monitoring. The threat actor interacted with TU/e systems and generated signals that could have led to earlier detection if the necessary monitoring systems had been onboarded into the SURFsoc service. The lessons learned section of this document lists specific opportunities for detecting and stopping this kind of cyberattack earlier.

Response

Saturday night

Phone call to FoxCERT

TU/e called the FoxCERT emergency phone number at 23:50 on Saturday, January 11, one hour after SURFsoc had escalated the incident to TU/e. FoxCERT had received a heads-up notification from SURFsoc. FoxCERT performed an intake call with TU/e at 0:15 on Sunday, January 12, assessed the situation, and provided immediate guidance for containing the attack and minimizing further damage. That guidance was in line with the actions already being taken by TU/e itself in response to the incident.

Immediate containment guidance

The urgent recommendations FoxCERT gave TU/e during the intake call were aimed at swiftly containing the threat and protecting digital assets from further compromise.

These included disabling internet connectivity to block remote access by the threat actor, preventing remote access via VPN, isolating possibly compromised systems to stop them from affecting the broader network, resetting various authentication mechanisms to reduce the risk of compromised credential material or accounts, and securing backups and verifying their integrity to ensure the feasibility of system and data recovery.

These containment measures matched and expanded upon the actions already being taken by TU/e as part of their internal response to the incident.

Network disconnected

At the time of the intake call at 00:15 on Sunday, January 12, TU/e had already isolated several systems and terminated VPN connections. Part of the guidance FoxCERT gave during that call was to disconnect the network from the internet and deny the threat actor remote access to university systems. An hour later, at 01:17, TU/e followed FoxCERT's guidance and disconnected its network from the internet. This strategic move aimed to block the threat actor's remote access and prevent further damage or data compromise.

This action proved successful, as no additional malicious activity was observed following the disconnection, indicating that the threat actor's access was indeed disrupted.

Boots on the ground

At 03:00 on Sunday, January 12, less than three hours after the intake call, FoxCERT incident handlers arrived onsite at TU/e to support the university and start the forensic investigation into the cyberattack, its scope and its impact.

TU/e staff had already been onsite since midnight and FoxCERT joined their ranks in the crisis response meeting held at 03:10.

The primary focus was to ensure that the cyberattack had been stopped and the threat actor could not continue any activities within the university's IT environment. Topics of discussion included the implementation of further containment measures and increasing visibility into TU/e IT systems.

Forensic investigation

Investigation goals

FoxCERT started its forensic investigation during the early hours of Sunday, January 12. The investigation was from the outset focused on supplying the TU/e crisis management team with the insights needed to recover and resume operations as soon as possible.The investigation aimed to determine the attack path used by the threat actor, including how they gained initial access and escalated privileges to domain administrator-level.

It also sought to identify which systems and accounts were compromised, the backdoors and other persistence mechanisms left by the threat actor, and whether data had been exfiltrated.

First week of investigation

The forensic investigation, conducted by FoxCERT in close collaboration with TU/e staff, revolved around collecting and analysing data from a multitude of systems throughout the TU/e IT environment. The multidisciplinary team of experts used specialized tools, such as Dissect, Splunk, and the Microsoft Defender suite, to collect data from over three hundred systems and other data sources, and construct an extensive timeline of events possibly related to the cyberattack.

FoxCERT and TU/e staff worked long hours throughout the week from Sunday, January 12, to Friday, January 17, iteratively expanding the scope and depth of their investigation. Each day they gained more insight into the cyberattack and were able to provide a progressively more complete and certain overview of its extent.

Supporting strategic decision making and communication

Throughout the investigation, FoxCERT collaborated closely with TU/e, sharing insights into the cyberattack and its scope as well as providing guidance and recommendations for recovery. Direct communication between FoxCERT and TU/e ensured a clear, shared understanding of the incident and allowed TU/e to manage the response and recovery efforts effectively, making decisions based on comprehensive situational awareness.

Scope of compromise

Compromised systems and accounts

FoxCERT investigated more than three hundred TU/e systems, revealing that the threat actor had interacted with 91 of these systems. The investigation uncovered evidence of manual activity by the threat actor on 14 of the 91 systems, while the remaining 77 systems exhibited only authentication activity without further interaction. This pattern aligns with common behaviour where threat actors gain access to numerous systems but selectively focus their efforts on a small number of targets to achieve their objectives swiftly and efficiently.

Additionally, the investigation identified five privileged accounts under the control of the threat actor.

Two of these accounts were newly created by the threat actor during the cyberattack, a common method used to maintain persistent, privileged access to an IT environment. The remaining three accounts were legitimate, existing accounts that the threat actor had compromised.

No evidence of large-scale data exfiltration found

Part of the investigation conducted by FoxCERT was a comprehensive search for evidence of data exfiltration by the threat actor.

This included searching for traces of data being collected and staged for exfiltration and examining the usage of known exfiltration tools, scheduled tasks, background services, system commands, and web browsing history related to data exfiltration.

It also included analysing Microsoft Defender data sources for indications of data exfiltration. None of these sources showed evidence of large-scale data exfiltration.

FoxCERT additionally analysed firewall logs provided by TU/e and network traffic data provided by SURF, which supplies network connectivity to TU/e and other higher education and research institutes in the Netherlands. This analysis focused on network traffic volume between TU/e systems and the internet. No patterns indicative of large-scale data exfiltration were identified.

Data that flowed to the threat actor

Although no evidence of large-scale data exfiltration was found, the investigation did reveal that some data flowed to the threat actor.

FoxCERT estimated that approximately 2 GB of data was transferred from TU/e systems to the threat actor. This volume is consistent with typical data flows resulting from technical cyberattack activities, such as interactions with remote systems and exploring systems and file shares on the network.

It is likely that this data contains sensitive technical information, such as Active Directory content, giving the threat actor detailed insight into internal systems and administrative configurations. However, this amount of data does not resemble the large-scale collection and exfiltration of sensitive data commonly used to extort victims of ransomware or data theft attacks.

Could the attack have been stopped without taking TU/e offline?
TU/e decided to take their network offline, effectively halting the cyberattack before it could cause further harm. When TU/e made that decision during the night of Saturday, January 11, and Sunday, January 12, there was not yet a complete overview into the extent of the compromise, making it difficult to remove the threat actor's access to the network and eliminate the threat with certainty at a granular level.

It was known that the threat actor had gained sufficient privileges to rapidly inflict significant damage, potentially stealing data and deploying ransomware. Based on the extensive experience FoxCERT has with similar incidents, taking the network offline was therefore the best decision available in that situation. The forensic investigation later confirmed that assessment of the imminent threat faced by TU/e.

Was it necessary to keep TU/e offline for a week?
Keeping the network offline for a week allowed TU/e and all involved parties, including FoxCERT, to concentrate fully on investigating the cyberattack and restoring the organization's security. Had TU/e brought the network back online sooner, the risk of the threat actor continuing their attack would have been significantly higher.

Additionally, the simultaneous tasks of investigating, recovering, securing the systems, and resuming normal operations would have divided the organization's focus, potentially prolonging the overall recovery process. FoxCERT therefore views the decision to keep TU/e offline for a week as an appropriate balance between reducing risk and reducing downtime.

Recovery

While the forensic investigation described in the Response section provided insights into the cyberattack, including how the threat actor gained access, which systems were compromised, and whether data was stolen, simultaneous recovery efforts were underway. These efforts restored affected systems so that TU/e could bring its network back online and resume normal operations as swiftly as possible.

FoxCERT worked closely with the TU/e incident response team and supplied the TU/e crisis management team with the insights to manage the incident. The response and recovery activities were closely related, with findings from the forensic investigation informing the recovery efforts. This pinpointed compromised systems and accounts, guiding the focus of TU/e recovery efforts and how best to remediate the damage caused by the cyberattack.

Cleaning up

FoxCERT supported TU/e throughout the recovery process. By analyzing compromised systems and identifying what the threat actor had done, they guided TU/e staff on the most effective methods to restore impacted systems and accounts to a known-good state, thereby minimizing future risks and preventing reinfection.

The forensic investigation revealed which systems had been compromised and how, ensuring TU/e could eradicate the threat actor from their environment before reconnecting the network and confidently resuming normal operations.

This iterative process involved continuous cooperation between FoxCERT and TU/e. Together they identified potentially compromised systems, which TU/e then provided access to or forensic data from.

FoxCERT investigated the systems and quickly fed back their findings to TU/e, informing the recovery activities and strategic decisions, and potentially expanding the scope of the investigation to include more systems.

To efficiently analyze hundreds of systems for signs of compromise while minimizing the risk of overlooked artifacts, such as hidden back doors, FoxCERT employed a combination of manual analysis and automated tools.

This approach provided detailed insights into the threat actor's actions on compromised systems and the best methods to clean and restore them to a secure state in preparation for going online and resuming operations.

To ensure the smooth execution of this rapid iterative process, FoxCERT and TU/e maintained close contact through direct communication channels like phone, chat, and email, as well as daily progress meetings.

Enhancing security

Beyond aiding in restoring systems to their pre-incident state, Fox-IT also helped TU/e strengthen its security posture through recommendations to harden systems and expanding the monitoring scope to significantly enhance detection capabilities compared to the pre-incident configuration. These recommendations and other insights derived from this incident are summarized in the lessons learned section of this report.

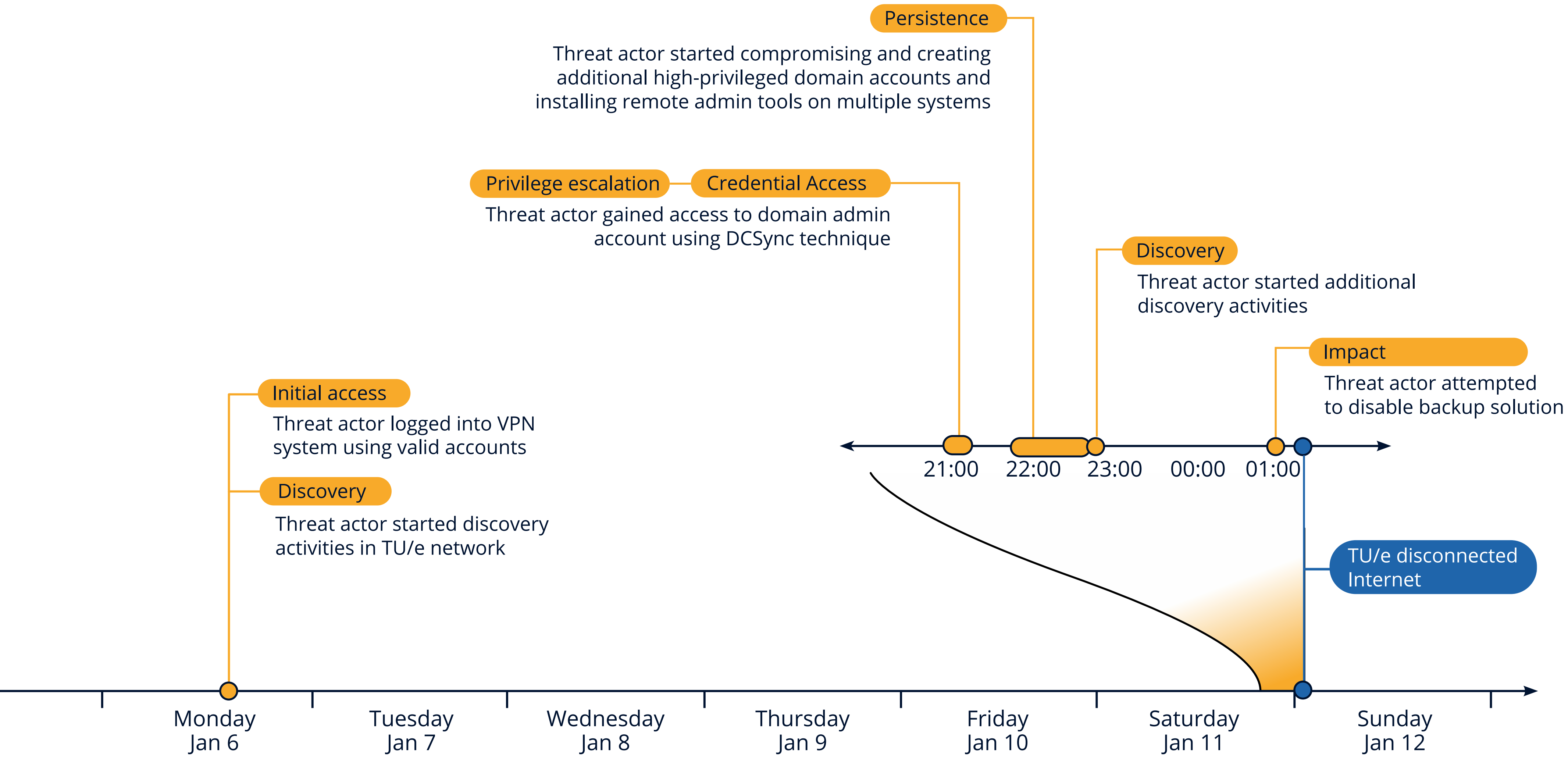
Additionally, offensive cybersecurity experts from Fox-IT's Red Team conducted a review from a threat actor perspective of certain TU/e systems, including their Active Directory, to identify potential weaknesses and support TU/e in addressing them efficiently.

Supporting decision-making and communication

FoxCERT's incident response support and forensic investigation provided TU/e with the necessary insights for strategic decision-making regarding recovery and the secure resumption of normal operations. As is typical during this kind of crisis situations, TU/e initially had to make urgent decisions under time pressure, including informing stakeholders and the public, based on incomplete information about the extent of the cyberattack.

FoxCERT and the rest of Fox-IT are proud to have supported TU/e throughout this event, swiftly delivering the insights needed for TU/e to confidently resume their education on Monday, January 20.

Reconstruction of the cyberattack



Persistence

Threat actor started compromising and creating additional high-privileged domain accounts and installing remote admin tools on multiple systems

Privilege escalation

Credential Access

Threat actor gained access to domain admin account using DCSync technique

Discovery

Threat actor started additional discovery activities

Impact

Threat actor attempted to disable backup solution

Initial access

Threat actor logged into VPN system using valid accounts

Discovery

Threat actor started discovery activities in TU/e network

TU/e disconnected Internet

This high-level reconstruction of the cyberattack summarizes key findings from the forensic investigation. It presents the sequence of actions performed by the threat actor, which FoxCERT was able to uncover retroactively by analyzing the available forensic sources.

First steps of the attack

Initial access

The threat actor connected to a VPN system hosted by TU/e on January 6. It used three different user accounts to connect; one of them failed but two succeeded. Those actions are the first activities that the forensic investigation linked to the attack with high confidence.

It is highly likely that the threat actor obtained credentials for the three user accounts from prior credential leaks available on the dark web. The VPN system was not configured to require multi-factor authentication (MFA), so valid usernames and passwords were sufficient for the threat actor to login successfully.

Initial discovery

Shortly after connecting to the VPN system, the threat actor started exploring the TU/e network. It connected to various other systems inside TU/e in a rapid fashion indicating the use of automated tools. This behaviour is similar to discovery activity that FoxCERT often sees threat actors perform soon after gaining access to a network.

Period of limited visible activity

The threat actor had access to the TU/e network via the VPN system for the five days between January 6 and January 11. However, during that period, the threat actor did not leave many forensic traces of activity.

The lack of evidence could suggest that the threat actor was inactive during this time. Alternatively, it may indicate that the threat actor was active in ways that were not visible to the security tools in place at TU/e. Specifically, at the network layer, there was limited data available for FoxCERT to investigate.

The VPN system provided network-level access to the TU/e network, potentially allowing the threat actor to perform actions that did not leave traces within the information available to the investigation.

Final hours of the attack

Privilege escalation

By the evening of Saturday, January 11, the threat actor had gained access to the system account of one of the TU/e domain controllers.

FoxCERT suspects that the threat actor obtained access to that account through a network-based attack technique known as a forced authentication coercion attack[1]. Based on the available information this could however not be confirmed.

At 20:00 on Saturday, January 11, the threat actor used that compromised system account to authenticate to a domain controller and attempt to access credentials and other sensitive information on that system using the DCSync technique[2]. That attempt failed.

An hour later the threat actor used that same compromised system account with a different domain controller and was able to successfully perform the DCSync technique. That effectively gave the threat actor domain administrator privileges and full control over the TU/e environment.

The threat actor subsequently changed the password of a dormant break glass account and configured it to be able to logon to other systems within the TU/e network. This break glass account, which existed as an emergency backup for situations where administrators could not use their regular accounts, held the highest level of privileges across the environment.

Further discovery

The threat actor used the break glass account to logon to various systems within the TU/e network and used three different tools to explore the environment, Advanced IP Port Scanner and SoftPerfect Network Scanner to scan the network and ShareFinder to search for file shares. This behaviour is similar to discovery activity FoxCERT commonly sees threat actors perform when planning the focus of their attack, possibly including data exfiltration and ransomware deployment.

Persistence

The threat actor used two distinct techniques to gain persistent access to the TU/e network: installation of remote administration tools and creation of highly privileged user accounts. AnyDesk and TeamViewer, two common remote administration tools, were installed on multiple systems providing the threat actor with remote access to those systems. The threat actor also created two new highly privileged user accounts, on top of the administrator accounts they had already compromised, through which they had complete administrative control over the TU/e domain.

The threat actor's control over remote administration tools and privileged accounts provides them with various methods to access and maintain their presence within the compromised TU/e environment. These techniques are commonly observed by FoxCERT as strategies used by threat actors to ensure prolonged access.

Attempt to disable backups

In the minutes before 01:00 on Sunday, January 12, the threat actor interacted with a backup solution used by TU/e and attempted to disable it.

Attack stopped by network disconnection

At 1:17, shortly after the threat actor's attempt to disable backups, the TU/e disconnected its network from the internet. That removed the threat actor's ability to communicate with systems inside the TU/e network and brought the attack to a standstill. No further activity related to this cyberattack was seen after the network was disconnected.

Who was behind the attack and what was their goal?

The cyberattack on TU/e exhibited many characteristics typical of a ransomware attack. The tactics, techniques, and procedures (TTPs), including the use of legitimate credentials for initial access, off-the-shelf tools and common techniques for network exploration, and a focus on obtaining high-level administrative privileges and extensive control over the TU/e environment, all align closely with those used by ransomware groups. FoxCERT has however not attributed the cyberattack on TU/e to a specific threat actor.

How advanced was this attack?

The cyberattack resembled a typical ransomware operation. The adversary employed widely known tools and techniques that indicate a reliance on readily available resources. The use of common tools and techniques suggests that the threat actor was of average to low sophistication, fitting the profile of many ransomware groups that prioritize efficiency and speed over innovation.

Lessons learned

Fox-IT hopes that by writing this report, containing insights into the cyberattack and the response process, the education sector and society in a broader sense can benefit and learn from it, helping to reduce the number and impact of future cyberattacks. By learning from this incident and implementing the recommendations outlined here, organizations can strengthen their security posture and better protect against future cyber threats.

Incident response and crisis management

TU/e demonstrated exemplary incident response and crisis management, responding rapidly and effectively even during the challenging hours of a weekend night.

This swift action serves as a model for other organizations. Key highlights include:

- Rapid response to SOC alert – TU/e quickly responded to the detection alert and initiated the incident response process promptly, even late Saturday night. The university's collaboration with SURFsoc and FoxCERT was smooth and efficient.
- Decisive action – The critical decision to bring the network offline was made under significant time pressure. This decision, though challenging given its impact on the university, was crucial in halting the cyberattack and preventing further damage.
- Dedication of staff – The commitment of staff members to respond to the detection alert and initiate the incident response process late Saturday night was commendable. Their dedication was pivotal in protecting the organization.
- Effective mitigation – The prompt actions taken likely prevented a more severe outcome, such as system encryption by ransomware, which would have complicated recovery and had long-term negative impacts on the university.
- Strategic-operational alignment – Continuous alignment was maintained between the incident response team (IRT) and forensic investigation at the operational level, and the crisis management team (CMT) and its strategic decision-making and communications at the strategic level.
- Communication – TU/e regularly communicated the status and progress of the incident to internal stakeholders and the wider public, even in the challenging situation where the investigation was still ongoing and situational awareness was far from complete.

Protect networks and remote access

Protecting networks and remote access is crucial to prevent unauthorized access and mitigate potential threats. Key insights from this incident include:

- Multi-factor authentication (MFA) – It is highly likely that in this incident the threat actor used valid credentials available on the dark web for initial access via the VPN system. Requiring MFA on all relevant systems, including that VPN system, would have acted as a significant barrier against the threat actor using compromised credentials to gain access.
- Network segmentation – This practice reduces the opportunities threat actors have for leveraging network connectivity in their attacks. It protects against network-based attacks, such as relay attacks and adversary-in-the-middle attacks, and it limits accessible communication channels between systems, reducing possibilities for lateral movement.

- Network monitoring – In the initial stages of the attack, evidence indicates that the threat actor utilized tools run on their own systems connecting into TU/e via the VPN system. This approach resulted in minimal traces of malicious activity on TU/e systems. It is highly likely that network monitoring, also known as network detection and response (NDR), would have detected these activities earlier at the network level.

Protect identities

Protecting identities is essential because abusing identities is an integral part of most modern cyberattacks. Key insights from this incident include:

- Multi-factor authentication (MFA) – Credentials found on the dark web typically include a username and password. MFA requires an additional form of verification and would have prevented the threat actor from authenticating to the VPN system with only a username and password. MFA is mentioned both here and under the section on network and remote access protection because it must be configured in both the Identity and Access Management (IAM) solution, such as Active Directory (AD), and the application, in this case, the VPN system.

- Online exposure monitoring (OXM) – It is highly likely that the threat actor used valid credentials available on the dark web for initial access via the VPN system. TU/e reports that an OXM tool the university uses had flagged the potentially compromised accounts several months prior. However, the follow-up actions left the passwords unchanged, thereby leaving them susceptible to exploitation.

- Identity monitoring – This incident clearly showed the threat actor's focus on compromising privileged accounts and using them to gain control over the IT environment. Monitoring for suspicious behaviour related to privileged accounts is crucial. Besides standard off-the-shelf monitoring, organizations should consider tailoring identity monitoring to detect unusual patterns in the context of their specific situation. Monitoring break glass accounts is an example of tailoring that Fox-IT regularly does for its clients. Because the configuration and usage of break glass accounts are specific to each organisation, such customization is only performed upon request and had not been done for TU/e.

- Securing IAM solutions – Identities are managed by IAM solutions, such as AD. Part of the support Fox-IT provided TU/e during the recovery process was a review of its AD configuration, uncovering several privilege escalation paths. Although the forensic investigation did not find evidence of these paths being exploited in this incident, their presence does pose a significant risk. Such vulnerabilities are frequently targeted by threat actors to gain administrative privileges and control over IT environments.

Protect backups

Backups are a core element in most disaster recovery strategies. As made clear by this incident, threat actors often target backup systems and try to disable them and make them unusable for recovery. It is therefore important to set up backup systems in ways that make them very difficult to attack and damage, ensuring they remain usable for recovery.

Role of SURFsoc

A Security Operations Center (SOC) such as SURFsoc plays a crucial role in stopping cyberattacks before they achieve their objectives, such as deploying ransomware.

SURFsoc can be viewed as a central security service that can support the protection of all different parts of an organization. For SURFsoc to provide that security value, it is important to connect SURFsoc to whatever systems are to be protected, ensuring it has the visibility and detection logic to be able to detect suspicious activity and respond accordingly.

Providing SURFsoc with comprehensive visibility and access to security tools is therefore essential. In this case implementing network monitoring would have provided SURFsoc (and the forensic investigation) visibility into the threat actor's network-level activities and likely the ability to detect the attack earlier. Additionally, fully integrating other security tools, such as Endpoint Detection and Response (EDR), into SURFsoc increases the likelihood of detecting and responding to cyberattacks effectively.

Sharing threat intelligence

Information about cyberattacks, including the tools and techniques used by threat actors and the vulnerabilities they exploit, is crucial for developing effective cybersecurity strategies. Sharing this information, known as threat intelligence, is important because it allows more organizations to benefit from the lessons learned.

Without sharing, each organization would only learn from its own mistakes, slowing progress towards a more secure society. This report exemplifies the commitment both TU/e and Fox-IT have to sharing the lessons learned from this incident with a broad audience, so everyone can benefit.

During the incident, TU/e and FoxCERT collaborated with SURFcert, sharing threat intelligence uncovered during the incident response and forensic investigation. Thanks to SURFcert's central role within the community of institutions affiliated with SURF, the threat intelligence from this incident was quickly disseminated and utilized by other higher education and research institutions to hunt for signs of compromise within their IT environments and validate their security.

Conclusion

The attack was detected at a critical moment, prompting swift action by SURFsoc, FoxCERT, and TU/e itself, leading to the decision to take the entire network offline. This rapid response halted the attack. The forensic investigation conducted by Fox-IT revealed that the attack exhibited many characteristics of a ransomware attack.

By stopping the attack, TU/e prevented exfiltration of large amounts of data and encryption. Consequently, the organization was not subjected to extortion or the need to pay ransom for a decryption key or to prevent data publication. This action minimized both financial and reputational damage.

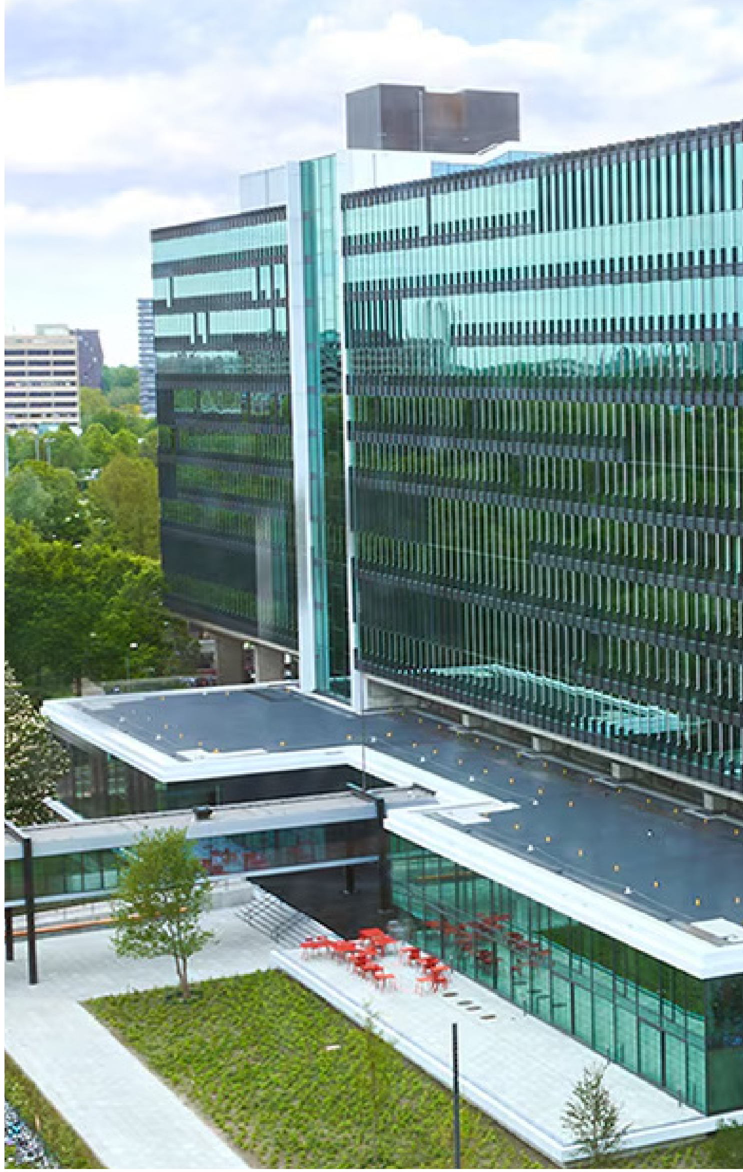
Despite the brief duration of the attack, it caused significant damage. The entire university was down for a whole week. Students and teachers, researchers and personnel had no access to its IT systems. The extent of this damage is difficult to quantify financially, but was clearly felt by all involved during and after the incident.

Although the cyberattack was stopped in time, many systems were compromised. A comprehensive forensic investigation was necessary to ensure the threat actor had not established means to regain access later. Only after confirming this could all systems be brought back online.

Fox-IT’s investigation uncovered how the cyberattack took place and provides important lessons to help organizations protect themselves. The report includes recommendations for strengthening security and highlights areas for improvement.

This case emphasizes the importance of effective cybersecurity, especially considering the inherent challenges faced by academic institutions such as TU/e. These include the large and dynamic number of students and staff with diverse needs, the high turnover rates of (student) users, the semi-public nature of a university, and the decentralized management structure that combines central services with significant autonomy for individual faculties.

We hope this report contributes to more informed decisions regarding security measures and fewer successful cyberattacks, not only for TU/e but also for the education sector and society as a whole.



FOX IT
part of nccgroup

Under attack?

Call our 24/7 Incident
Response hotline.

INT: +31 88 369 23 78
NL: 0800 369 23 78