NORTHWAVE
Intelligent Security Operations

NORTHWAVE
YOUR MOST IMPORTANT DIGITAL THREATS

THE THREE MOST SERIOUS FORMS OF CYBERATTACKS TODAY

DISSECTED AND EXPLAINED THROUGH EXAMPLES

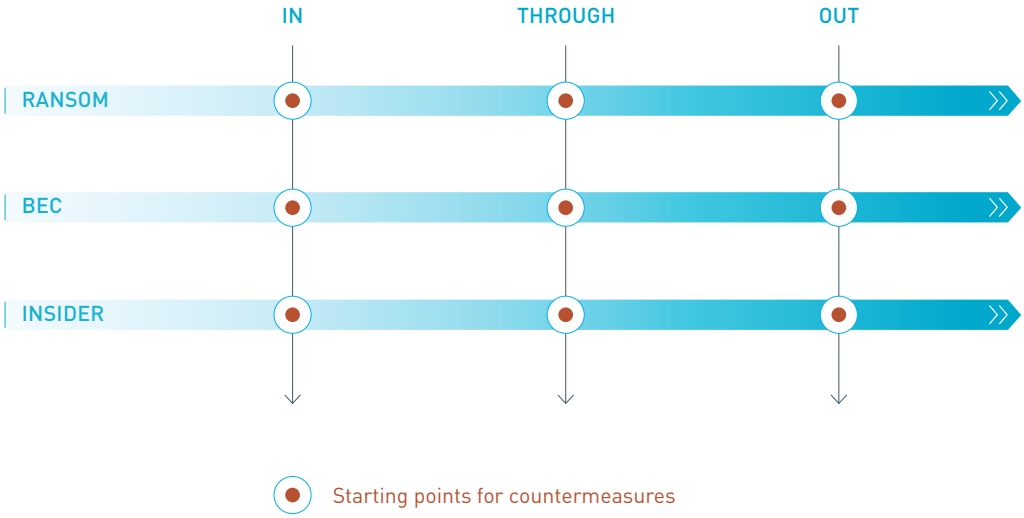
INTRODUCTION

One moment, nothing seems to be amiss, and the next, the realisation hits home. All files have been encrypted. A large sum of money has been transferred to a stranger. Company secrets or customer data are out in the open.

Every day, all sorts of companies and institutions experience the disproportionate impact cybercrime can have. Business failure, reputational damage, financial damage—not every company or institution can overcome this kind of blow.

Very often, cybercrime is relatively easy to prevent. But first, you need to know how attacks work. Only then can you make the right risk assessments and the right investments to stop them. For that reason, we describe in the coming pages the three most serious threats today using practical examples. We break them down into phases and explain in understandable language what happens in each phase.

This document consists of two parts. First, the practical examples are described and outlined according to the model below; then, each one is discussed in more detail.



RANSOMWARE

His attack was rejected by the virus scanner three times. The fourth time, the attacker succeeded. The next morning, the IT department was buzzing with calls—no one could access their data any more. The company had come to a screeching halt.

BUSINESS E-MAIL COMPROMISE

Using a well-targeted email, the attacker managed to trick the purchasing manager into providing his login details. A week later, half a million dollars was transferred to the attacker's bank account.

INSIDER

A week after a merger was announced, a director out for a day on the golf course received a threatening email. Confidential information was in the hands of an unknown individual, and that person had a few demands.

CYBERATTACKS IN A SIMPLE MODEL

CYBERCRIME AFFECTS EVERYONE

Society is continuing to digitise, and crime is following in this trend. While classic crime seems to be declining, losses due to cybercrime continue to grow year after year. Companies and institutions increasingly rely on digital resources. The failure of these resources, their unreliability or their falling into the hands of third parties can have disastrous consequences. Your company can become a victim of this as well.

Cybersecurity is often seen as an intangible, invisible world that the Board thinks it knows too little about. A cost instead of an investment. An attitude of 'it won't happen to me' has already cost many company leaders their heads. The experts agree on this: for cybercriminals, every organisation is a potential source of income or data. The question is not whether, or even when, they will try to attack. Attempts take place continuously. The question, therefore, is how well-armed you as a company are against such attacks.

RISK MANAGEMENT INSTEAD OF TECHNOLOGY

Cybersecurity is not vague, distant or complicated. In essence, it is a risk assessment. You want to know how big the chance is and what the damage would be of cyberattacks. And then you want to protect your systems sufficiently there where it is needed. To do this, it is important to first have an idea of how attacks work. That is what we will discuss here.

We take three cyberattacks, describe them and then analyse them. We also look at several variants. We have chosen ransomware, business email compromise and insider attacks because the first two are the most frequently occurring types, and the third can have the greatest impact. The descriptions are based on real-world cases. These examples and the chosen variants provide insight into approximately 90 to 95 per cent of current cyberattacks.

When dissecting, we divide the attack into three phases, in accordance with the most widely used scientific models. We call these phases IN, THROUGH and OUT.

IN	THROUGH	OUT
The actions the attacker takes to successfully penetrate the digital environment.	The actions the attacker takes to navigate the digital environment.	The actions the attacker takes to achieve their ultimate goal.
AN EXAMPLE		
Boris breaks the kitchen window and enters the residence.	Boris follows a path through the house from the attic to the bedrooms to the living room, searching through closets and drawers.	Boris steals all the electronic devices and leaves the building.

RANSOMWARE

DESCRIPTION

Ransomware is malicious software that encrypts a victim's systems or files; after encryption, the key is offered in exchange for payment. Ransomware can have a significant impact on the continuity of your business operations. Therefore, the financial consequences often go far beyond the payment of ransom.

THE REALISATION

It is 6:30 on Monday morning. As always, Jan-Jaap is the first one at the office. He starts up Word but gets a message that the last file opened no longer exists. How can that be? He checks his personal directory on the file server and sees that all the files have a strange extension. He also finds a ransom.txt file. It says that all the files are being held hostage and refers him to a TOR site for further instructions.

THE CASE

In the past, The Stock Foundation made use of the Confluence application. This software was accessible from the internet. The program was no longer actively used but had not been removed either. Confluence had had a recent security bug that made it possible for attackers to run commands on the underlying system via the application. The vulnerability had recently been patched, but The Stock Foundation was running an older version of the program. Just over a month after the vulnerability was announced, The Stock Foundation was attacked through the Confluence vulnerability.

Because Confluence was running with domain administrator rights, the attacker could easily reach most of the servers in the network through the Confluence server. He copied the database and installed a known ransomware tool on the servers, but the antivirus program recognised this and blocked it. The attacker then tried a new type of ransomware, which was not detected. He infected other systems in the network through the Confluence server and destroyed the backups. He disabled the antivirus software. Then he encrypted the files. System information was sent to a computer controlled by the attacker to later enable decryption. Finally, the attacker left a ransom note—a message containing payment instructions for the victim.

The Stock Foundation was not the only company affected by this attack. The attackers had scanned the internet for vulnerable systems and had almost completely automated the attack.

IMPACT: The Stock foundation paid €230,000 (10% of its profits) to the attackers. The systems were down for two weeks during a busy time. With external help, the phased restoration of the systems took another three days. All systems were then checked to see whether all traces of the malware were gone. Finally, the company invested heavily in security.

IN	THROUGH	OUT
Scan of the internet for vulnerable Confluence servers connected to the internet. Exploitation of a vulnerability to access Confluence server.	Access as many servers as possible through Confluence server. Delete backups. Install and activate ransomware. Ransomware encrypts all files.	Copy of database. Ransom note.

HOW IT COULD HAVE BEEN

The previous example concerns only one of the possible scenarios. The same is true of the following examples. In practice, every attack is different. It is therefore important to also consider the variants.

Below, using the example given, we give alternatives for each of the three phases of IN, THROUGH and OUT. We have limited ourselves to the forms that we regularly encounter, so this is not an exhaustive list. The method used in the example always comes at the top.

IN

Exploitation of a vulnerability in a server connected to the internet.

Ready-made tools are often available for known vulnerabilities.

Phishing email.

An email with a malicious attachment or link. These emails can be tailor-made and are therefore almost impossible to distinguish from authentic emails.

Remote-access software—vulnerable password.

If login can take place via the internet, attackers can attempt to guess the password.

THROUGH

Lateral movement: spreading through the network (through vulnerable systems or insufficient access controls).

The attacker hops from computer to computer.

Privilege escalation: Becoming Admin by password guessing, unsafe user rights settings or vulnerabilities.

The attacker attempts to secure more user rights on a computer, thereby gaining increased access.

Lateral movements and privilege escalation can be deployed in tandem.

Deletion of backup files.

OUT

Encryption of files and demand for ransom.

The attacker unleashes a cryptographic function on files—the key needed to undo this has to be purchased from the attacker.

Sensitive data downloaded—threat to publish.

Company-sensitive or personal data are stolen from the server. The victim has to pay to avoid publication.

Easy to combine with encryption.

BUSINESS EMAIL COMPROMISE

DESCRIPTION

Business email compromise (BEC) is a form of fraud in which the attacker manipulates the email traffic between two parties to execute fraudulent transactions. BEC can result in a considerable financial impact and a significant reputational damage for organisations.

THE REALISATION

Roger Eumann, Head of Purchasing at Daricross NV, is just about to switch off his computer to go home when he gets a call from Marthe Meulens from the Finance Department.
She is quite upset. 'If you could ask me nicely and professionally from now on.' Roger has no idea what she is referring to—he has not spoken to her in a while. Marthe tells him that she has just made a large payment at his insistence.

THE CASE

Daricross is in the process of converting from a local Exchange server to Microsoft 365. Much of the company has already been migrated; Roger Eumann has not. On a Sunday, Roger receives a message that Microsoft 365 has quarantined five emails. They will be deleted if he does not act immediately. The message contains a link, and Roger uses this to log into his account. Subsequently, however, nothing happens.

The legitimate looking message was a phishing attempt. Roger gave away his login details to an attacker. The attacker logged into the Outlook Web App that same week and copied all of the emails in Roger's account. The attacker's Mac also receives all new emails from this point on. The attacker starts a program that automatically scans the ongoing email conversations for keywords indicating upcoming financial transactions. In the meantime, he reads up on who's who in the company.

After just two days, Roger receives an invoice from a foreign business partner, and the attacker makes his move. The attacker replaces the account number with a Singaporean account number under his control. Using Roger's email, he asks Marthe Meulens from Finance to pay the bills without delay.

The attacker archives all the emails on the subject so that Roger does not see them. On one occasion, the attacker does not do this on time, and the real Roger enters the conversation and asks what is going on. The attacker intervenes and removes Roger from the conversation.

Due to a typo, the transfer fails and has to be made again. The attacker turns up the heat and sends a barrage of emails in Marthe's direction. Thanks to the bank's help, the payment is still made that day. After the discovery, Daricross tries to get their money back—but it is too late.

IMPACT: Daricross transferred €435,817.33 to a foreign bank account.

IN	THROUGH	OUT
Phishing email lures Roger into disclosing his login details.	The attacker uses this to log in and then copies and reads Roger's email. The attacker then forces his way into an email conversation in which he pretends to be Roger.	Marthe transfers funds to the attacker's account.

HOW IT COULD HAVE BEEN

As with the ransomware case, we will once more use the previous example to present a number of alternatives for the three phases. The methods used in the example are again listed first. Note that the same methods (such as phishing emails) can be used for different forms of cybercrime.

IN

Phishing email.

An email with a malicious attachment or link. These emails can be tailor-made and are therefore almost impossible to distinguish from authentic emails.

Remote-access software—vulnerable password.

If logging in can take place via the internet, attackers can attempt to guess the password.

Registration of a domain name that bears a strong resemblance to the victim's domain name in order to impersonate the victim.

Creation of an email address that looks like that of the victim.

THROUGH

Downloading and reading of email.

After access, emails can be synchronised and read.

Email is monitored for financial discussions.

This is frequently an automated process done based on keywords that indicate financial transactions.

Email contact lists in order to take over more accounts.

The attacker can attempt to garner more victims through the contact list.

OUT

Manipulation of invoices.

Existing invoices are intercepted, modified and resent with another bank account number.

Altered bank data is sent.

The attacker sends (in the name of the victim) a message to third parties indicating that they need to update the bank account number in their administration. If this attempt is successful, then there are two victims.

Invoices are produced.

The attackers create invoices and attempt to get them paid.

These can also be fake invoices from a personal email address.

INSIDER

DESCRIPTION

By insider, we mean someone with legitimate access to the environment. The fact that the person is already inside makes defending against these types of attacks more difficult. Malicious insiders are relatively rare but can significantly impact business operations continuity, reputation and/or finances. The motive is often resentment or anger but can also be financial. In addition, insiders sometimes unintentionally cause damage.

THE REALISATION

It is Saturday morning, and Healthnomic director Pam Tikkenberg is on the golf course when her phone rings. It is fellow director Martin van Sluis, asking her whether she has read her email this morning. She has not. It turns out that a threatening email has been sent to both directors, and it has information that should only be known to them. In the email the sender threatens to publish all intellectual property on the Pastebin website.

THE CASE

Healthnomic has a merger in the works, and employees are worried about being made redundant. The IT department, in particular, would supposedly be on the bad end of the deal. Henk Mortix decides to put a stop to this. As an IT employee, he already has access to the company environment and has more access rights than the average employee. He also knows how the network works.

Henk spends a week collecting the contents of all the email boxes and the shared and personal folders of every Healthnomic employee. He copies them to his own external drive. Then, he creates an anonymous ProtonMail email address. From this address, he sends an email on behalf of Anonymous with an ultimatum: a resignationfree merger or all that data will be made public.

Management starts up an investigation, but Henk gets wind of it. He proceeds to publish.

IMPACT: All the company data, including Healthnomic's intellectual property, is out in the open and now in the hands of the competition. As a result, the merger fails. Six months later, the company is bankrupt.

IN	THROUGH	OUT
Henk is in already: as an employee he has access to the environment.	Henk grants himself access to the email environments and the shared and private files of colleagues.	Henk copies sensitive company data and sends a threat. Henk publishes the company data.

HOW IT COULD HAVE BEEN

For this scenario, too, we give a number of alternatives for IN, THROUGH and OUT. In one of the alternatives, OUT is in turn INput for another form of cybercrime. This is not unusual.

IN

Job application.

The insider may have been hired long ago and become dissatisfied over time or have been drawn into a criminal organisation.

A contractor with physical access to elements of the digital environment.

In principle, an outsider but with inside access to carry out maintenance, etc.

THROUGH

Lateral movement.

Gaining access to data not relevant to the execution of the individual own tasks.

Privilege escalation.

Gaining access to data which should not be accessible to that individual.

OUT

Collection of data and subsequently damaging it or rendering it useless.

Destruction or encryption of company data for the purposes of revenge, etc.

Selling or sharing of data.

The stolen data may be used during an interview, posted on the internet or sold on the dark market.

IN

Criminal organisation uses this data as the starting point for a cyberattack.

INSIDER

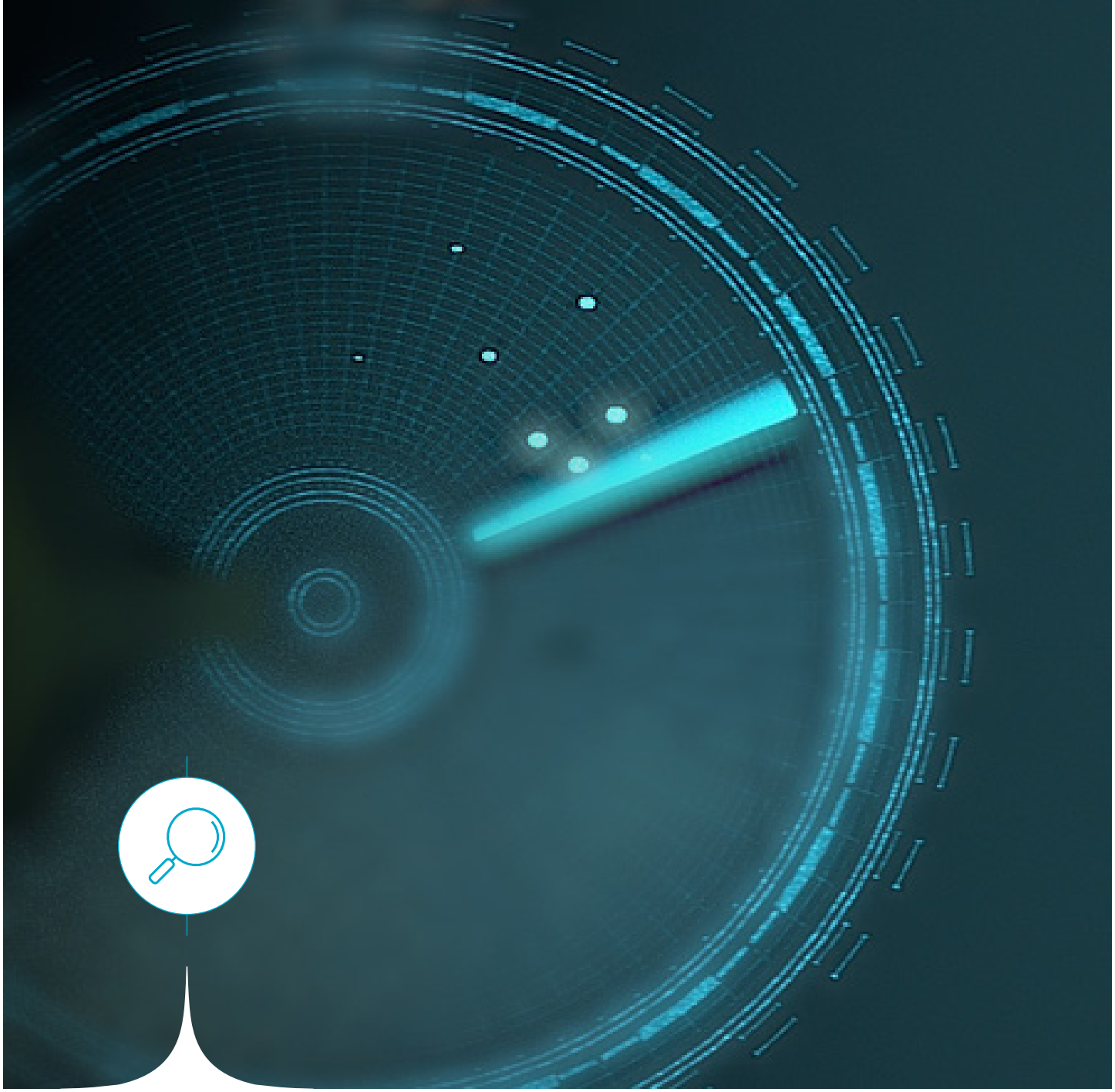
THE TECHNIQUES IN A ROW

In the examples just given, we have seen that there are different variants of attacks and that different techniques are used. Yet we have also seen that the same technique can be used in different attacks. For that reason, we list the different techniques for IN, THROUGH and OUT again here.

Understanding the techniques used in the different phases provides starting points for defence.

IN	THROUGH	OUT
Phishing emails. (potentially from a tailor-made domain)	Lateral movement. Privilege escalation.	Encrypting data and demanding ransom.
Remote access software—vulnerable password.	Observing and learning. Snooping in the environment or reading emails.	Stealing and publishing data or threatening to publish data. Stealing and selling data.
Exploiting a vulnerability on a server connected to the internet.	Automatic monitoring of network environment or emails.	Manipulating data, e.g. invoices.
Insider: already in.	Using victim email to garner more victims.	Destroying data.
Trusted contractor: granted access.		Using systems for other purposes, e.g. crypto currency mining, botnets (not mentioned earlier).

A CLOSER LOOK



THE UNIFIED KILL CHAIN

ONE LEVEL DEEPER

The preceding examples provide good insights into the three phases of the most serious digital threats today. In the following pages, we will deepen this understanding by looking at the IN, THROUGH and OUT phases of the examples in greater detail. This in turn provides points of departure for defensive measures.

Northwave uses the Unified Kill Chain as a model to provide insight into attacks.

DESCRIPTION

Paul Pols proposed the Unified Kill Chain in 2017 as a derivative of Lockheed Martin's Cyber Kill Chain®, the MITRE ATT&CK framework and a few other models. It divides cyberattacks into 18 unique steps—but not every step is taken in every attack. The steps are divided into 3 phases, which we refer to here in simplified terms as IN, THROUGH and OUT.

Here, we give a brief overview of the attack steps in the Unified Kill Chain and explore the three examples in greater depth, each in their own way, to gain a better understanding of the phases.

IN

INITIAL FOOTHOLD
Compromised System

The actions taken by the attacker to successfully penetrate the network.

- Reconnaissance
- Weaponization
- Delivery
- Social Engineering
- Exploitation
- Persistence
- Defensive Evasion
- Command & Control

THROUGH

NETWORK PROPAGATION
Internal Network

The actions taken by the attacker to navigate the network.

- Discovery
- Privilege Escalation
- Execution
- Credential Access
- Lateral Movement

OUT

ACTION ON OBJECTIVES
Critical Asset Access

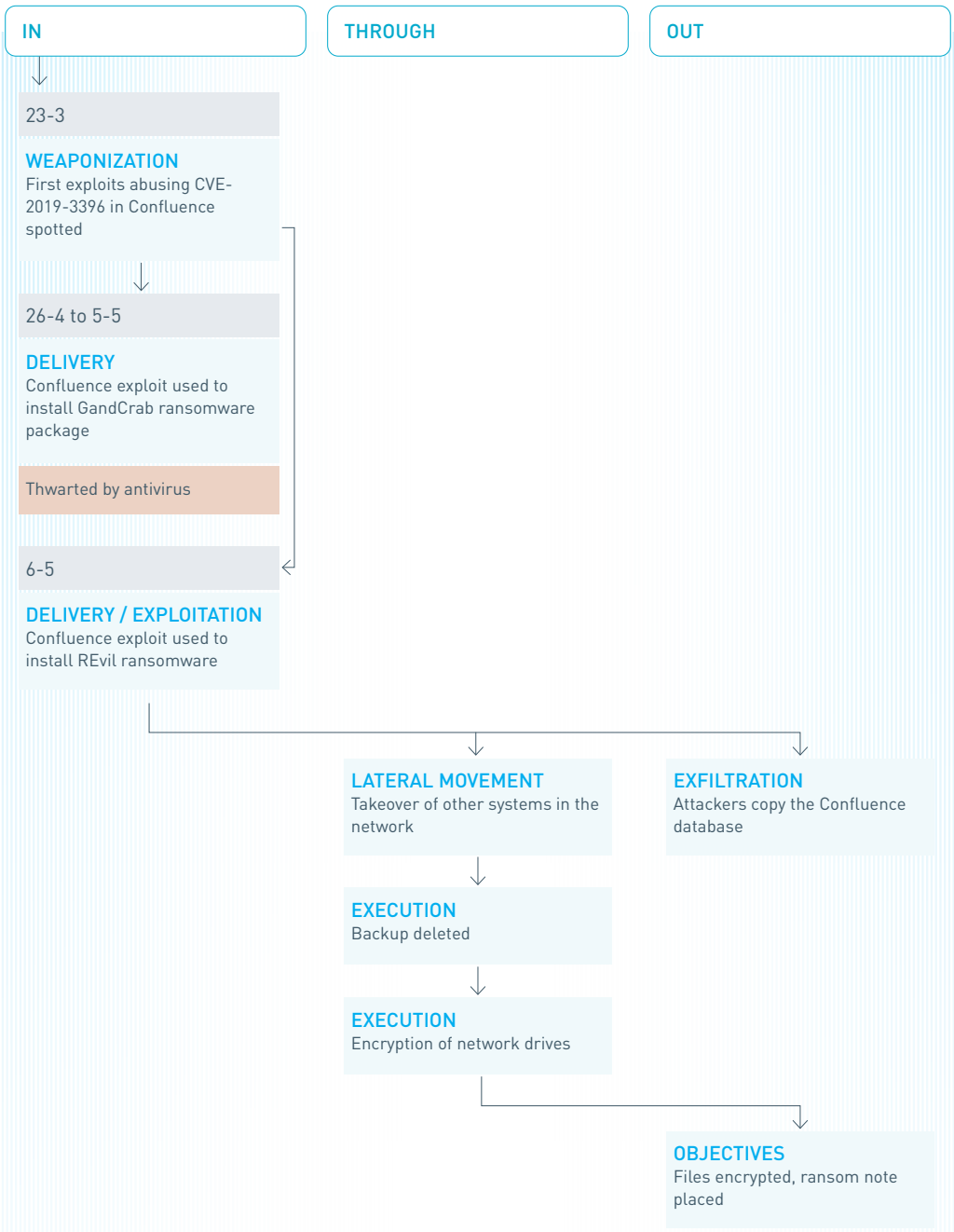
The actions taken by the attacker to achieve their ultimate goal.

- Collection
- Exfiltration
- Target Manipulation
- Objectives

LINKS

https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain-Thesis.pdf
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
https://attack.mitre.org/

RANSOMWARE



A CLOSER LOOK

RANSOMWARE

BEFOREHAND

5 March 2019		Bugfix release for all versions due to a vulnerability in Atlassian Confluence found in 2018.
20 March 2019		CVE-2019-3396 published: vulnerability allowing attackers to execute Java code with user rights of the person who started Confluence.
23 March 2019	Weaponisation	The first attacks in the wild that exploit the vulnerability in combination with GandCrab ransomware.
		- The Stock Foundation is running an old version of Confluence with a vulnerability on the SF-INTRANET-01 internal server. - Confluence is started with system administrator rights.

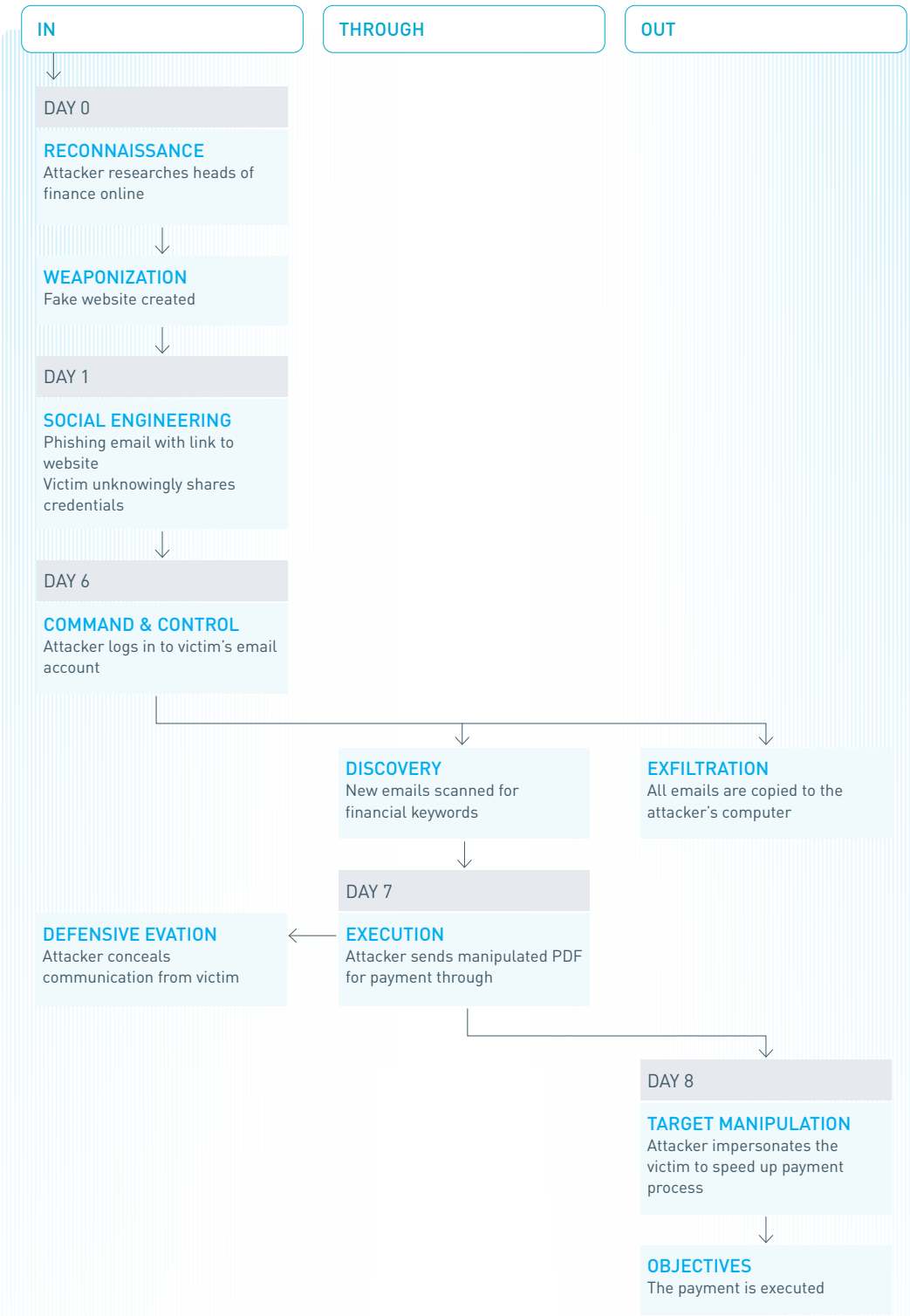
26 APRIL TO 5 MAY: FAILED ATTACKS

26 April 2019 - 5 May 2019	Delivery	The attackers gain automated access to the Confluence server four times during this time and try to install GandCrab ransomware. This is blocked by antivirus software.

6 MAY: SUCCESSFUL ATTACK

0:27	Delivery	The attackers again gain automated access to the Confluence server.
0:50	Exploitation	REvil ransomware replaces GandCrab. REvil is first seen very shortly before this attack and is not yet recognised by virus scanners. SF-INTRANET-01 downloads and installs REvil.
1:17	Exfiltration	The attackers copy the Confluence database to an unknown location via the internet.
1:21	Lateral Movement	The attackers look for and infect as many other servers and workstations as possible from SF-INTRANET-01.
1:26	Execution	The ransomware deletes all Volume Shadow Copies. These are files that Windows creates in order to go back to previous versions of a file.
1:28	Execution	The attackers have found and taken over the backup server. They give the command to delete all backups.
1:31	Execution	The encryption command is executed for all files and folders on all drives accessible from the infected computers.
1:31 - 9:50	Objectives	The files in 6710 folders are encrypted, and a ransom note is placed in each folder. The SF-INTRANET-01 desktop is also modified and supplied with a ransom note.
6:30		Jan-Jaap starts up Word and cannot open his files.
9:50		The Stock Foundation disconnects from the internet.

BUSINESS EMAIL COMPROMISE



A CLOSER LOOK

BUSINESS EMAIL COMPROMISE

DAY 0: PREPARATION

	Reconnaissance	The attacker scours the internet for buyers and heads of finance and collects email addresses and company information.
	Weaponisation	The attacker goes live with a fake Microsoft365 site with the aim of capturing login data from victims.

DAY 1: THE ATTACK (FRIDAY)

19:19	Social Engineering	The attacker sends a spam message to Roger Eumann. It looks like a valid Microsoft365 message saying that some emails have been quarantined and action is required. The link under the action button leads to the site run by the attackers.
19:20	Social Engineering	Roger opens the email and clicks on the button. Entering his login details does not take him to the expected quarantine page. He assumes that something went wrong technically. He tries again at 21:24 and 23:02.

DAY 3: FIRST DEFENCE (SUNDAY)

10:27	Social Engineering	Roger tries again, but in the meantime, SafeLinks has marked the link as malicious and has blocked it.

DAY 6: EXPLOITATION (WEDNESDAY)

00:26	Command & Control	The attacker logs into Roger's account. He does this via OWA (Outlook Web) on a Mac using the login data obtained on day 1.
19:20	Exfiltration	Outlook for Mac synchronises with Roger's email box—Roger's entire email history is now in the hands of the attacker.
19:25	Discovery	The attacker sets up an email rule that scans Roger's email for a list of keywords that could indicate a financial transaction. If one of these words appears, the attacker is alerted.

DAY 7: THE MANIPULATION (THURSDAY)

14:01		Roger receives an email from a foreign business partner that includes two invoices. The attacker receives a signal.
15:01	Command & Control	The attacker logs into Roger's account via webmail.
15:02	Defensive Evasion	It removes the email in question from the server.
15:24	Execution	The attacker forwards the original email to Marthe with a payment request. He has altered the PDFs in the process. The payment details on the first two pages have been replaced by a foreign bank account under the attacker's control.
15:24	Defensive Evasion	The attacker sets up an email rule that hides the conversation between Roger and Marthe from the real Roger.
15:44		Marthe replies that the payments will go out the next day and asks for confirmation, which the attacker gives shortly afterwards.

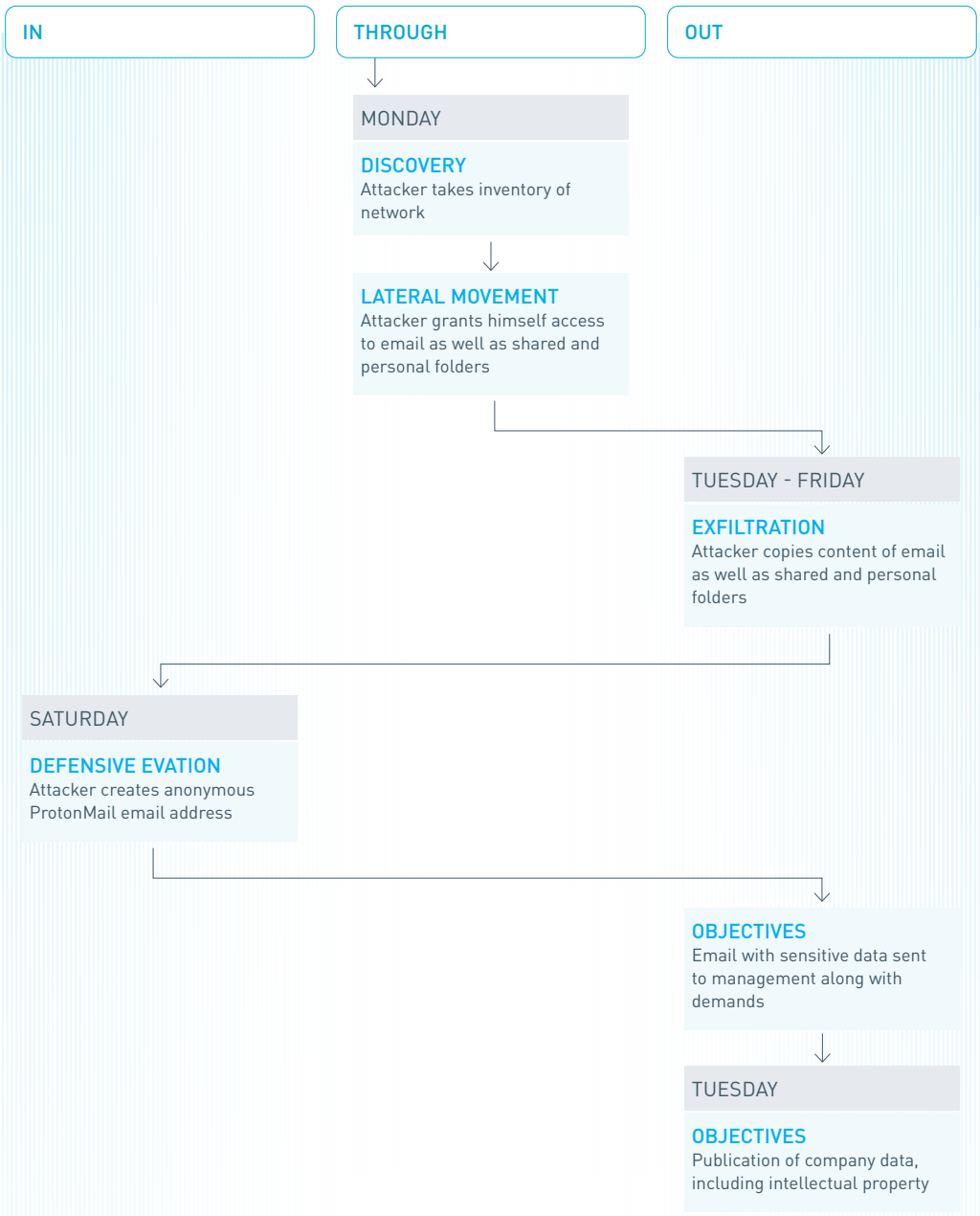
BUSINESS EMAIL COMPROMISE

DAY 8: THE PAYMENT (FRIDAY)

11:45	Target Manipulation	Marthe requests a SWIFT message from the bank by email for verification purposes. She also indicates that there is a typo in the name of the addressee.
11:50	Target Manipulation	The attacker intervenes in this conversation and sends several emails in the hours that follow.
14:32	Mistake by the attacker	The real Roger Eumann gets involved in the discussion. The attacker has forgotten to set up an email rule that hides messages from the bank. Roger inquires what this is about.
14:36	Defensive Evasion	The attacker sets up a new email rule that also hides bank emails from Roger.
14:38	Defensive Evasion	The attacker avoids suspicion by immediately sending an email after Roger's and removing Roger from the email conversation.
15:27	Objectives	The bank sends confirmation of the transfer.
15:37		The attacker thanks the bank.

A CLOSER LOOK

INSIDER



A CLOSER LOOK

INSIDER

BEFOREHAND

Friday, 7 July		The management of Healthnomic announces an upcoming merger and indicates that redundancies may be the result.

THE ATTACK

Monday, 10 July	Discovery Lateral Movement	Using his administrator rights, Henk grants himself access to Emails as well as shared workspaces and personal folders of colleagues and management.
Tuesday to Friday	Exfiltration	Using his administrator rights, Henk grants himself access to email boxes, shared workspaces, and colleagues and management's private folders.
Saturday, 15 July	Defensive Evasion	Henk copies the contents of these email boxes and folders to a private hard drive.
Saturday, 15 July	Objectives	Henk creates an anonymous ProtonMail email address.
Tuesday, 18 July	Objectives	Henk sends an email to management with sensitive information and his demands.

A CLOSER LOOK