The Cyber Force LDCE

presents

C.I.P.H.E.R.

Cyber Incident Profiling & Hazard Evaluation Report

SECURING DIGITAL WORLD

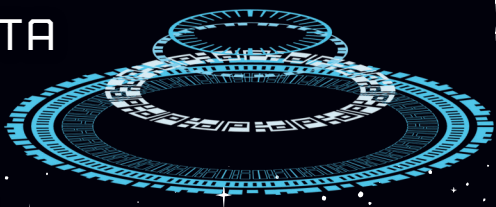
Ensuring the cyber security, one Byte at a Time.

ILOVEYOU BREACH

THE LOVE LETTER THAT INFECTED MILLIONS

TARGET DATA BREACH

WHEN SHOPPING TURNED DANGEROUS



THE INOTIV BREACH

HOW QILIN RANSOMWARE CRIPPLED A PHARMACEUTICAL GIANT

SCAN HERE

Oct - Jan '25/ Volume 1

The Cyber Force LDCE

ILOVEYOU BREACH

The Love Letter That Infected Millions

$10B	45M+	10%	<24 Hrs
Financial impact	Computers infected	World's PCs hit	Global spread

In May 2000, an email with subject line "ILOVEYOU" spread globally at unprecedented speed. Created by a Filipino programmer, it contained an attachment labeled "LOVE-LETTER-FOR-YOU.txt.vbs", a Visual Basic Script disguised as a text file.

Once opened, it destroyed critical files including photos and documents, then automatically sent copies to every contact in the victim's Microsoft Outlook address book. The emotional appeal made people click without thinking, a perfect social engineering.

The attack succeeded because users didn't understand file extensions-".vbs" looked harmless. Microsoft Outlook lacked safeguards against self-replicating scripts. Windows Script Host ran with full privileges, giving complete system control.

The worm overwrote files, installed hidden scripts in startup folders, and sent stolen credentials to attacker-controlled emails. Within days, it crashed email servers worldwide, disrupting businesses and governments across continents.

LOVEYOU caused $5-10 billion in damages globally. Despite tracing the attack to the Philippines, no prosecution occurred,the country lacked cybercrime laws. This prompted worldwide cybercrime legislation. Microsoft blocked dangerous extensions and disabled automatic script execution.

Anti-virus companies developed behavior-based detection. Most importantly, it awakened the world to social engineering threats. Today's security awareness training exists because of lessons from this attack, proving human psychology is the weakest security link.

The Cyber Force LDCE

TARGET DATA BREACH

When Shopping Turned Dangerous

$200M+	110 M	70 M	41 M
Financial impact	Customers impacted	Records exposed	Payment Cards stolen

The Target breach did not begin inside Target's own systems. Instead, threat actors executed a **supply-chain attack**, first compromising a **third-party HVAC vendor** responsible for heating and cooling systems across Target stores. That vendor possessed **legitimate credentials** for routine network access.

Once stolen, these credentials became a digital master key, allowing attackers to bypass perimeter defenses and infiltrate Target's internal network undetected. From there, the intrusion rapidly escalated.

Using the compromised credentials, attackers conducted lateral movement across the network and deployed malware on point-of-sale (POS) systems nationwide. The POS malware was engineered for stealth, capturing payment card data directly from system memory at the moment of each transaction, before encryption could occur.

The stolen data was then exfiltrated in real time to attacker-controlled servers. There were no system crashes, no visible disruptions, and no immediate indicators for store employees or customers.

The malware captured payment card data directly from system memory at the moment of each transaction–before encryption could occur–and quietly exfiltrated it to attacker-controlled servers.

Normal store operations continued without disruption, delaying discovery. By the time the breach was uncovered, 41 million payment cards and 70 million customer records had been compromised.

The Cyber Force LDCE

THE INOTIV BREACH

How Qilin Ransomware Crippled a Pharmaceutical Giant

176GB	162K+	4 Days	9542
Data Stolen	Files compromised	Attack window	Victims affected

In August 2025, Inotiv Inc., a $500 million pharmaceutical research company, was attacked by the Qilin ransomware gang. Between August 5-8, threat actors infiltrated the company's networks, encrypting critical systems, and stole 176 GB of data.

The breach exposed personal information of 9,542 individuals, including Social Security numbers and medical records, alongside proprietary research files, financial documents, and lab reports dating to 2018.

Qilin, the second most active ransomware group with 482 victims in 12 months, gained access through spear-phishing or by using stolen passwords bought from the dark web. Once inside, attackers deployed PowerShell-based NETXLOADER malware ,gained full system access using security flaws, and disabled antivirus protection.

They then steal data using file transfer tools and encrypt everything with military-grade locks (AES-256), deleting shadow copies and wiping event logs to eliminate recovery options.

Inotiv engaged cybersecurity specialists and transitioned to offline operations. Systems were restored by December 2025, nearly four months post-attack. Affected individuals received 24-month credit monitoring. The attack exposed serious gaps: poor network protection, delayed detection giving hackers days to work, and weak backup systems.

Qilin later removed Inotiv from their public victim list, suggesting ransom payment. This shows why pharmaceutical companies are prime targets, holding valuable research and sensitive personal data.

SNIPPETS

Your mini dictionary for hacking terms

- **Social Engineering**: The psychological manipulation of users into trusting, clicking, or opening malicious content, often by exploiting emotions such as curiosity or urgency.
- **Supply-Chain Attack**: A cyberattack where hackers breach a trusted third party to gain access to a larger, secured organization.
- **Spear-phishing** : A trick attack where hackers pretend to be someone you trust to fool you into clicking links or sharing passwords.
- **Malware** : Malicious software designed to steal data, damage systems, or disrupt operations.

FUN FACTS

- **PowerShell**, a normal Windows tool, is used in over 40% of file-less attacks because it looks harmless.
- Scripting languages like VBS, PowerShell, and JavaScript are widely used by attackers because they are built into operating systems and often trusted.
- Modern cyberattacks increasingly rely on legitimate system tools, making them harder to distinguish from normal activity
- Over 60% of major breaches begin with stolen or weak credentials, not malware exploits.

Puzzle Zone: Cyber Edition

R	I	H	I	E	P	I	N	R	H	I	T	P	N
R	A	P	A	N	T	L	A	I	C	R	R	R	O
L	N	N	O	T	O	R	W	C	A	I	C	N	I
I	L	E	S	W	A	T	L	E	E	E	T	C	T
P	N	S	I	O	E	R	I	F	R	A	F	I	P
H	R	R	R	O	M	R	G	V	B	A	I	T	Y
I	M	I	P	A	R	W	S	E	R	C	R	C	R
S	S	O	C	I	A	L	A	H	T	P	E	E	C
H	I	L	T	A	A	A	A	R	E	L	W	A	N
I	R	I	T	O	E	N	R	L	E	L	A	E	E
N	L	M	A	L	W	A	R	E	L	L	L	S	C
G	E	R	E	T	N	C	F	R	I	N	L	L	E
T	C	R	E	D	E	N	T	I	A	L	S	P	E
B	O	T	N	E	T	L	E	R	A	Y	R	S	A

NOTE : Answers will be posted on our instagram page within 2 days.

The Cyber Force LDCE

About C.I.P.H.E.R.

CIPHER is a student-driven online cybersecurity magazine that breaks down real cyber incidents, explaining how attacks happen and why systems fail -making cybersecurity simple, relevant, and impactful for everyday readers.

About TCF LDCE

The Cyber Force (TCF) is a student-led tech community focused on cybersecurity and emerging technologies. We aim to spread awareness, encourage learning through real-world insights, and build a culture of secure and responsible digital innovation.

Samveg Shah — President

Ibrahim Madakiya — Chairman

Asmita Rathod — Secretary

Design By
Arth Doshi

Research By
Virti Gandhi