# WannaCry

## Summary

WannaCry is a type of ransomware that was first discovered in May 2017. It spread rapidly and infected more than 200,000 computers in 150 countries within a few days. The ransomware demanded payment in Bitcoin in exchange for unlocking the victim's files and threatened to delete them if the payment was not made. The attack caused widespread disruption, including to healthcare organizations, government agencies, and businesses.

## Details

WannaCry was first discovered on May 12, 2017, and was spread via a worm that exploited a vulnerability in the Microsoft Windows operating system. The vulnerability, known as EternalBlue, was discovered by the United States National Security Agency (NSA) and was leaked by a group known as the Shadow Brokers. The worm was able to spread quickly because many organizations did not update their systems with the necessary security patch.

Once a computer was infected, the ransomware encrypted the victim's files and displayed a message demanding payment in Bitcoin. The ransomware also had a worm component that allowed it to spread to other vulnerable computers on the same network. The attackers behind the ransomware have not been identified.

## MITRE ATT&CK TTPs

The following table shows the MITRE ATT&CK TTPs that WannaCry used:

|  |  |  |  |
| --- | --- | --- | --- |
| Tactic | Technique ID | Technique Name | Procedure |
| -------- | ------------- | ---------------- | ----------- |
| Initial Access | T1190 | Exploit Public-Facing Application | The attackers used the EternalBlue vulnerability to exploit a public-facing SMB port on the victim's system. |
| Execution | T1027 | Obfuscated Files or Information | The ransomware used obfuscated code to evade detection by antivirus software. |
| Execution | T1059 | Command-Line Interface | The attackers used the command-line interface to execute the ransomware and other tools. |
| Persistence | T1060 | Registry Run Keys / Startup Folder | The ransomware created a registry entry to ensure that it would execute on system startup. |
| Defense Evasion | T1218 | Signed Binary Proxy Execution | The attackers used a signed binary to execute the ransomware, which allowed it to bypass some security measures. |
| Defense Evasion | T1027 | Obfuscated Files or Information | The ransomware used obfuscated code to evade detection by antivirus software. |
| Credential Access | T1003 | Credential Dumping | The attackers used the Mimikatz tool to dump credentials from the victim's system. |

## Indicators of Compromise

The following table shows the known indicators of compromise for WannaCry:

|  |  |  |
| --- | --- | --- |
| Type | Value | Description |
| ------ | ------- | ------------- |
| File Hash | 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c | WannaCry ransomware executable |
| File Hash | ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa | WannaCry ransomware executable |
| IP Address | 212.47.232.237 | Command and control server |
| IP Address | 217.79.179.177 | Command and control server |
| Domain Name | iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com | Kill switch domain used to stop the spread of the ransomware |