Ransomware: a correlation between infection vectors and victims

Doina Cosovan, Catalin Valeriu Lita, Jue Mo, Ryan Sherstobitoff

Virus Bulletin 2021
Ransomware Infection Stages

- Initial access
- Local operations
- Data exfiltration
- Data encryption
- Ransom payment or data leakage
Ransomware Leaks Websites

Conti

DoppelPaymer

REvil

Malcolm C Foy & Co Limited

https://www.malcolmfoy.co.uk/

Malcolm C Foy & Co is a leading firm of solicitors in South Yorkshire with offices in Doncaster and Rotherham having been established since 1972. We are renowned as a trusted advisor to our clients, which include both individuals and...
Ransomware leaks per month

This chart shows the number of ransomware leaks per month from January 2020 to May 2021. The number of leaks increases significantly in some months, particularly in 2020-09 and 2021-05.
Ransomware leaks March-May 2021

The chart shows the distribution of ransomware leaks for different strains over the months of March, April, and May in 2021. The y-axis represents the number of leaks, while the x-axis lists various ransomware strains: Conti, Avaddon, REvil, Babuk, DarkSide, DoppelPaymer, LV, Marketo, Clop, and Prometheus. The bars for each strain indicate the number of leaks in March (blue), April (red), and May (yellow).
Digital Footprint
Initial Access

- Exposed services
- Vulnerabilities
- Spam
- Leaked Credentials
- Application Security
- Malware Infections
Initial Access: Exposed Services
Initial Access: Abused Services
Use Case: SSH Brute Forcing

SSH brute forcing on April 7 between 7 AM and 12 AM

Leak appeared on website on May 30
Use Case: RDP

- RDP brute forcing between March 25 and March 30
- RDP exfiltration between April 25 and April 30
- Leak appeared on the website on June 3
Initial Access: CVEs with POC
Initial Access: RCE CVEs
Initial Access: Spam
Initial Access: Leaked Credentials
Initial Access: Application Security
Initial Access: Malware from sinkholes

![Bar chart showing malware types and affected companies](chart.png)
Initial Access: Ransomware related malware from netflow
Trickbot infection

- Trickbot connections to C2 between May 18 and May 27
- Leak appeared on website on May 20
Lateral Movement
Lateral movement: Cobalt Strike

![Bar chart showing lateral movement through Cobalt Strike in different companies and ransomware. The chart compares the number of companies affected by different ransomware types, with Cobalt Strike being most prominent.]
Exfiltration
REvil exfiltration to Mega over HTTPS

Connections to 3 Mega IP addresses on March 21 between 3 AM and 3 PM

Leak appeared on website on April 26
LV exfiltration to Rackspace over SMB

Connections to Rackspace IP addresses over SMB between April 8 and April 13

Leak appeared on website on April 19
DarkSide exfiltration to Digital Ocean over SSH

Connections to 1 Digital Ocean IP address over SSH on May 6

Leak was made public on May 8
Post Leak Exfiltration
Recommendations

- **Credentials**: don’t reuse credentials, use strong passwords, use a password manager, use Multi Factor Authentication, don’t make your phone number and email address easily accessible.

- **Exposed services**: minimize the exposed digital footprint, use strong authentication where applicable, put services behind VPN where applicable.

- **Vulnerabilities**: patch them immediately especially if they provide Remote Code Execution or Privilege Escalation and if there is a publicly or commercially available proof of concept.

- **Malware**: use an up-to-date Anti-Malware product.

- **Exfiltration**: use an Intrusion Detection System (IDS) / Intrusion Prevention System (IPS) / Firewall, monitor for and block large outgoing amounts of data.
Conclusions