

# HOW MALWARE INFILTRATES THROUGH THIRD-PARTY SOFTWARE



As companies look to third parties for specialty services, digital ecosystems become expansive and complicated. Malware continues to be a popular tactic to manipulate third parties and gain entry into corporate networks.

## COMMON THREATS

Today's attackers have more opportunities and a myriad of tactics like malware to break into organizations.



**ADVANCED PERSISTENT THREATS**

Motives: Geopolitical, Financial


Targets: Damage, Disruption, Data Theft



**CRIMINAL**

Motives: Financial

Targets: Data Theft, Ransom



**INSIDER**

Motives: Retaliation, Financial, Accidental

Targets: Damage, Disruption, Data Theft



**HACKTIVIST**

Motives: Political

Targets: Disruption, Damage



**RESEARCHER**

Motives: Safety, Interest

Targets: Data Theft

## NOTABLE TACTICS & TECHNIQUES

Actors are seeking new entry points into single organizations, leveraging today's complex digital ecosystems and supply chains, delivering malware across multiple areas, including:



Display advertising



Browsers



Software Development Kits



Outdated Software



Legacy Hardware



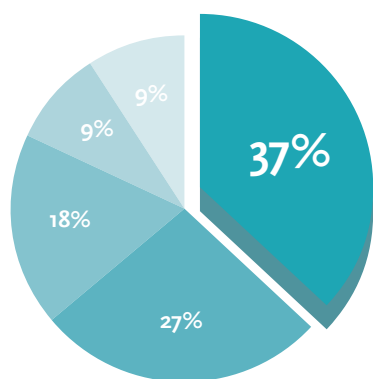
Open Source Tools



### IT COMPANIES & SOFTWARE PROVIDERS

- Auto update servers third party network connections
- Mobile software development kits
- Enterprise software used for command-and-control communications
- Steganography tools

Emotet was among the most frequently detected by Booz Allen targeting the IT sector between December 2018 and April 2019.



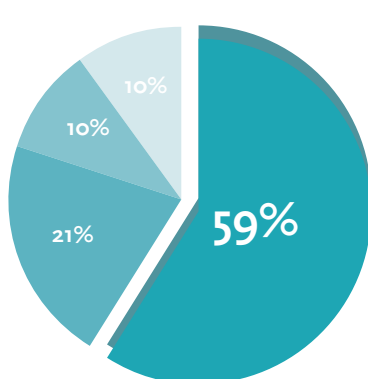
Emotet, Dridex, Qakbot, Kovter, Install Core



### FINANCIAL SERVICES & BANKING INSTITUTIONS

- Compromised third parties
- Enterprise software
- Domain hijacking

Booz Allen Managed Threat Services Intel found that 89 percent of all observed threats to the financial industry between February and April 2019 were email based, with 66 percent of those emails containing malicious links.



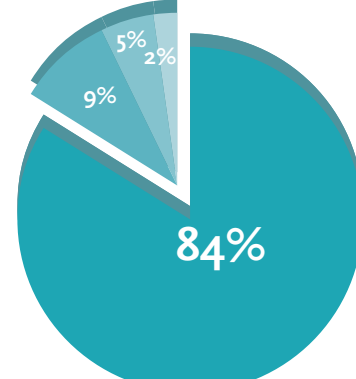
Emotet, Hawkeye, Adwind, Install Core



### RETAIL

- eCommerce sites
- Enterprise software used for command-and-control communications
- Steganography tools

Retail industry is targeted with the most diverse range of malware types, including ransomware, remote access trojans, and keyloggers.



Emotet, Ursnif, Formbook, Other

## GAINING DEEPER VISIBILITY IS KEY TO PREVENTION & REMEDIATION

Adopting a more cohesive understanding of cyberthreats with a consolidated monitoring capability provides visibility into cyber threats faster and uncovers complex attack chains.



Threat Hunting



Open Source Tools Analytics



Third-Party Supplier Vetting



Patching



Managed Detection and Response