ThreatCure

Cyber Threat Advisory

AKIRA

Threat Actor Ransomware

CATEGORY

Ransomware

SEVERITY

High

Platforms

Windows & Linux

IMPACT

- Data Loss
- High costs for ransom, recovery, and fines.
- Business disruptions and productivity loss.

Description

AKIRA

The Howling Scorpius ransomware group, emerging in early 2023, is behind the Akira ransomware-as-a-service (RaaS), which has become one of the most active ransomware groups globally. Leveraging a double extortion strategy, the group exfiltrates critical data before encryption, threatening to leak stolen data if victims refuse to pay. It primarily targets small and medium-sized businesses across various industries in North America, Europe, and Australia, including education, manufacturing, and government. Howling Scorpius maintains encryptors for both Windows and Linux, including variants for ESXi hosts, and continuously enhances its toolset, increasing the risk for organizations.

Howling Scorpius affiliates use methods like exploiting vulnerable VPNs, spear phishing, and targeting remote services for initial access. They employ tools like Mimikatz and LaZagne for credential theft and adopt advanced evasion tactics, such as creating malicious drivers and disabling security tools. The group uses a Tor-based leak site to list victims and share stolen data, further pressuring compliance. Victims receive ransom notes with links to negotiation sites and unique codes for communication. Akira's ransomware encryptors are capable of targeted encryption and shadow copy deletion, making it a significant threat to businesses worldwide.

Kill Chain

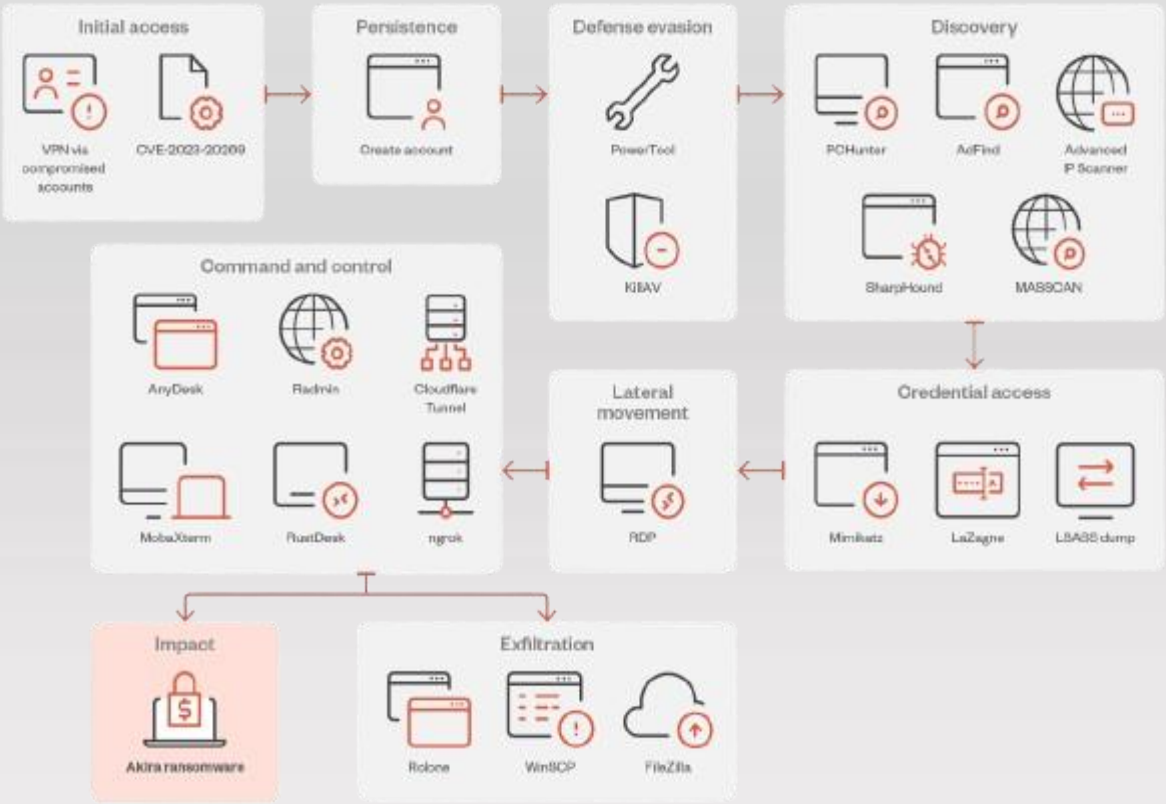

Figure 1 Kill Chain

Indicator of Compromise

SHA256

```
08207409e1d789aea68419b04354184490ce46339be071c6c185c75ab9d08cba
2727c73f3069457e9ad2197b3cda25aec864a2ab8da3c2790264d06e13d45c3d
2db4a15475f382e34875b37d7b27c3935c7567622141bc203fde7fe602bc8643
56f1014eb2d145c957f9bc0843f4e506735d7821e16355bcfbb6150b1b5f39db
58e9cd249d947f829a6021cf6ab16c2ca8e83317dbe07a294e2035bb904d0cf3
678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33
1ba1ccfacffbb6be9480380f5535a30d3eee1dd7787f3c649ebf8ea2a6a5de51
9f873c29a38dd265decb6517a2a1f3b5d4f90ccd42eb61039086ea0b5e74827e
1b6af2fbbc636180dd7bae825486ccc45e42aefbb304d5f83fafca4d637c13cc
cc970bd2673e46c7e0df5430ab617bc2a9214b4d5c2c44252af681a08ff526a8
131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07
28cea00267fa30fb63e80a3c3b193bd9cd2a3d46dd9ae6cede5f932ac15c7e2e
2f629395fdfa11e713ea8bf11d40f6f240acf2f5fcf9a2ac50b6f7fbc7521c83
68d5944d0419bd123add4e628c985f9cbe5362ee19597773baea565bff1a6f1a
7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be
95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a
9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f23d065
9f393516edf6b8e011df6ee991758480c5b99a0efbfd68347786061f0e04426c
a6b0847cf31ccc3f76538333498f8fef79d444a9d4ecfca0592861cf731ae6cb
b55fbe9358dd4b5825ce459e84cd0823ecdf7b64550fe1af968306047b7de5c9
c0c0b2306d31e8962973a22e50b18dfde852c6ddf99baf849e3384ed9f07a0d6
c9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b3898b0
dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198
e3fa93dad8fb8c3a6d9b35d02ce97c22035b409e0efc9f04372f4c1d6280a481
1d3b5c650533d13c81e325972a912e3ff8776e36e18bca966dae50735f8ab296
300bc2769c6d62ba9d228cc45e126cd458e1a23fd23092da258053afd82f2755
3805f299d33ef43d17a5a1040149f0e5e2d5db57ec6f03c5687ac23db1f77a30
3999a25f8f0fd8252aa9250fa9bd70aae202f181812cc6c230c8ea2842340f18
3dc7d4023c7380ed740ac5ac7d82a4ba6f587f430b2b7b66f1d34a44f89c39cb
43c5a487329f5d6b4a6d02e2f8ef62744b850312c5cb87c0a414f3830767be72
6005dcbe15d60293c556f05e98ed9a46d398a82e5ca4d00c91ebec68a209ea84
74f497088b49b745e6377b32ed5d9dfaef3c84c7c0bb50fabf30363ad2e0bfb1
7ca3e6b4dd4d98506faa92ab590108cacb2945b8c27dcf1ac75b0df4a206493a
```

Indicator of Compromise

MD5

```
cb9c73b52474adb4a24a2a17daa2b95a
7ca94d84f4a02fb1f608818c1c3ab62d
b6162bebd1daab783d85c498721c60ff
71ab9950464359366b9d96c9f576a468
b3e63badb7006dfe9602ce6fb876cb90
d25890a2e967a17ff3dad8a70bfdd832
b666ea987c7dff545e984ad88ce80a9b
34ad4ab24152c2bca2a4aa23f847c4d1
0c30fdc297c54753166d572ed04d1d6b
4edc0efe1fd24f4f9ea234b83fcaeb6a
0e98bfb0d8595ceb9a687906758a27ad
64f8e1b825887afe3130af4bf4611c21
bd046164daf3c30e265d4f9c6647f630
a18d79e94229fdf02ef091cf974ed546
9f801240af1124b66defcd4b4ae63f2a
e5cf95b6bd04b89447e6c4ed71105a1c
3f63951399f8cd578e2a6faed2c9c0f0
6036b0acaa33423b73b26c3be854cb84
06e493f1f9a620ecec1a4f32fedd3128
eb2479d710d08cffec1ad42bc1edc7aa
9df999f142f137b0794b8afcaaedc588
fd380db23531bb7bb610a7b32fc2a6d5
b0a59e8b365962c73da486bccc361354
302f76897e4e5c8c98a52a38c4c98443
a0f2727dd11b0f5ced13eadc3d5bba73
d68a565f1a5962ea081a212b2e7c36e2
43351ce424c9a72fcb47de7da7b368c3
825620363d5ff8e4d820a402bfcb425d
8ef468f21842ee03e1c5a41a6fef6bba
913ad33912e8d074a44010b9f6380969
2acf0461cb310ad4109cce68e4c07afe
bd3350d018170b7f45ea7ec5375f534e
```

Remediation

- Regularly back up critical data and store it offline.
- Apply security patches promptly to eliminate vulnerabilities.
- Strengthen email security and train employees to identify phishing.
- Enforce least privilege access and implement multi-factor authentication (MFA).
- Use endpoint protection tools like EDR or XDR to detect ransomware activities.

ThreatCure

Cyber Threat Advisory

Secure your byte world

AKIRA

Threat Actor Ransomware

Get Started Today

For more information about the ThreatCure ShieldOps Platform or to schedule a demo, please contact:

- Website: www.threatcure.net
- Email: info@threatcure.net

THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE