■侵入の痕跡（Indicators of Compromise、IoC）

Description	Hashes/URLs/IP Addresses	Detection Name
Revised invoice 2 .pdf	c59ac77c8c2f2450c942840031ad72d3bac69b7ebe780049b4e9741c51e001ab	Trojan.PDF.POWLOAD.AM
2021-08-09_220350.pdf.pdf	5a586164674423eb4d58f664c1625c6dfabcd7418048f18d4b0ab0b9df3733eb	Trojan.PDF.POWLOAD.AM
shipment assessment.pdf	fb7fe37e263406349b29afb8ee980ca70004ee32ea5e5254b9614a3f8696daca	Trojan.PDF.POWLOAD.AM
LOA.PDF.pdf	98983e00b47bcbe9ebbaf5f28ea6cdbf619dd88c91f481b18fec7ffdb68ab741	Trojan.PDF.POWLOAD.AM
Bunker invoice 023.pdf	71998bb4882f71a9e09b1eb86bac1e0a0ac75bc4c20ee11373b90173cedc7d0b	Trojan.PDF.POWLOAD.AM
PO JHS-PO-2108-11425.rar-1.pdf	e5d84990d7abd7b65655ac262d3cad346cdaf47f5861bff8b33b8bc755832288	Trojan.PDF.POWLOAD.AM
N/A	2210000d2f877c9fd87efe97605e90549c5d9008a90f9b062a570fc12437e318	Trojan.W97M.LOKI.AOR
Contract 1459-PO21-15.docx	e7a518b83d9f57a4cb8726afc6bb27a15f6e68655552e13b24481df83b9320fb	Trojan.W97M.LOKI.AOR
PI I229-I231.xlsx	fc5bf62f57c77efa9f9264878f1753a35c27fb44bce7d9a00f8f094315355661	Trojan.X97M.CVE20180802.AL
S28BW-421072010440.PDF.xlsx	c6aede79cc1608da1e3ed5c8853b1718351429573679d6b847c90c44e48137d4	Trojan.X97M.CVE20180802.AL
64DBB078907CDEB6E	639f6453e961aa33302d34962ccdd29fbc9235b2a0df8b1ac0acc0bb040af7e0	Trojan.W97M.LOKI.AOT
76CE5B8A21BB98A.mlw		
PO20-003609.xlsx	b1b0045f890afd14b4168b4fc0017ac39c281fe5eee66d3c9523040e63220eb4	Trojan.X97M.CVE201711882.XQUOOYI
rwer.wbk	3798eb011f5d8ee7f41e3666dac7fac279cf670ad	Trojan.W97M.CVE2017

	4af4060aaef33a7def3c6f7	11882.XAAAAEG
pdf_r34567888.html	45f1b4b0a627f1a2072818d00456dc4fc6607edf9a1a1c484f04f800d25b93d2	Trojan.HTML.POWLOAD.EQ
pdf_rg234999233.html	da56c38fad7c2ee8e829aea9bd3c4b523ea0b65e935805d68df12c7a28e5d5dd	Trojan.HTML.POWLOAD.EQ
vbc.exe	d8bb1bb8587840321e74cf2ab2f3596344cbb5ffeb77060bd9aade848fed03fd	TrojanSpy.Win32.LOKI.PUHBAZCLQR
vbc.exe	9f66135d831d5ba4972ba5db9e0fd4515dfaecc92013a741679d6cddbe29ab25	TrojanSpy.Win32.LOKI.PUHBAZCLQR
vbc.exe	324d549fb7b9999aa0e6fb8a6824f7a05fe5f1f21d76fb2d360cb34c56eb1995	TrojanSpy.Win32.LOKI.PUHBAZCLQR
vbc.exe	ca155beb7d28cde5147eba7907c453d433b7675ba1830e87d5a4e409b5b912e1	TrojanSpy.Win32.LOKI.PUHBAZCLQR
URL	http://198[.]23[.]212[.]137/document/pdf_document_s233322[.]html	Phishing
URL	http://198[.]23[.]212[.]137/document/pdf_document_sw211222[.]html	Disease Vector
URL	https://ulvis[.]net/Q4gl	Disease Vector
URL	https://ulvis[.]net/Q4km	Disease Vector
URL	http://198[.]23[.]212[.]137/document/pdf_rg234999233[.]html	Disease Vector
URL	http://198[.]23[.]212[.]137/document/pdf_r34567888[.]html	Disease Vector
C&C IP Address	198[.]23[.]212[.]137	C&C Server
C&C IP Address	104[.]21[.]62[.]89	C&C Server
C&C IP Address	104[.]21[.]71[.]169	C&C Server
C&C IP Address	185[.]227[.]139[.]5	C&C Server
C&C IP Address	46[.]173[.]214[.]209	C&C Server
C&C IP Address	192[.]227[.]228[.]106	C&C Server

TREND MICRO ™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information. Our innovative solutions provide our customers with layered security for data centers, cloud workloads, networks, and endpoints.

At the heart of our leadership, Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights with the public, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on targeted attacks, artificial intelligence, Internet of Things (IoT), cybercriminals, and more. We continually work to anticipate the next